대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 특허출원 2003년 제 0065249 호
Application Number 10-2003-0065249

출 원 년 월 일 : 2003년 09월 19일
Date of Application SEP 19, 2003

출 원 인 : 주식회사 아이앤아이맥스
Applicant(s) INIMAX Co., Ltd.

2004 년 10 월 1 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【출원일자】	2003.09.19
【발명의 명칭】	네트워크상의 장비들 간의 통신제어방법 및 이를 위한 장치
【발명의 영문명칭】	Method of controlling communication between equipments on a network and apparatus for the same
【출원인】	
【명칭】	주식회사 아이앤아이맥스
【출원인코드】	1-2003-035070-5
【대리인】	
【성명】	박희진
【대리인코드】	9-1998-000233-1
【포괄위임등록번호】	2003-064164-6
【발명자】	
【성명의 국문표기】	신용만
【성명의 영문표기】	SHIN,YONG MAN
【주민등록번호】	640718-5100188
【우편번호】	463-833
【주소】	경기도 성남시 분당구 정자동198-2/5 정든마을 613-1205
【국적】	KR
【발명자】	
【성명의 국문표기】	송석칠
【성명의 영문표기】	SONG,SEOK CHUL
【주민등록번호】	650805-1023927
【우편번호】	138-160
【주소】	서울특별시 송파구 가락동 161-3 현대5차아파트 51동 1501호
【국적】	KR
【발명자】	
【성명의 국문표기】	신용태
【성명의 영문표기】	SHIN,YONG TAE

【주민등록번호】 661013-1475724

【우편번호】 156-030

【주소】 서울특별시 동작구 상도동 중도빌라 나동 103호

【국적】 KR

【발명자】

【성명의 국문표기】 주용준

【성명의 영문표기】 JU,YONG JUN

【주민등록번호】 680118-1535244

【우편번호】 435-040

【주소】 경기도 군포시 산본동 세종아파트 632-2404

【국적】 KR

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 박희진 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	40	면	40,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	16	항	621,000 원

【합계】 690,000 원

【감면사유】 소기업 (70%감면)

【감면후 수수료】 207,000 원

【첨부서류】 1. 요약서·명세서(도면)_1통 2.소기업임을 증명하는 서류_1통

-

【요약서】

-

【요약】

본 발명은 네트워크 내부 장비들에 대하여 통신 허용 또는 통제 등에 대한 통을 제함으로써 네트워크 내부 장비들 간에 가상의 방화벽이 존재하는 것과 같은 환경 구축할 수 있게 하는 방법과 장치를 개시한다. 이를 위한 통신제어장비는 네트워 상의 다른 장비들과 동일 레벨에 위치한다. 이 통신제어장비를 이용하여, 통신차 대상인 장비들에 대하여 데이터링크 레이어 어드레스가 조작된 ARP 패킷을 제공하 차단대상 장비가 송신한 데이터 패킷이 비정상적인 어드레스로 전송되도록 한다. 에 의해 차단대상 장비들 간의 통신이 차단된다. 통신차단의 대상이 아님에도 불구 고 통신차단상태에 있는 장비에 대해서는 통신제어장치가 정상적인 어드레스 정보 내포하는 ARP패킷을 해당 장비에게 송신함으로써 그러한 통신차단상태를 제한다.

대표도】

도 2

【명세서】

【발명의 명칭】

네트워크상의 장비들 간의 통신제어방법 및 이를 위한 장치 (Method of trolling communication between equipments on a network and apparatus for the e)

【도면의 간단한 설명】

본 발명의 실시예에 관한 상세한 설명은 첨부하는 도면을 참조하여 이루어질 것며. 도면에서 대응되는 부분을 지정하는 번호는 같다.

도 1은 본 발명에 따른 통신통제방법을 구현한 시스템 구성예이다.

도 2는 LAN(40)에 연결된 망내 장비들에 대한 통신을 제어하는 본 발명에 따른 법을 개략적으로 도시한다.

도 3은 통신제어장치 EQ-X가 망내 두 장비 EQ-1과 EQ-2 간의 통신을 통제하는 을 설정하는 방법을 도시한다.

도 3은 통신제어장치 EQ-X가 망내 두 장비 EQ-1과 EQ-2 간의 통신을 통제하는 에 따른 패킷 흐름의 제어 방법을 도시한다.

도 4는 에이전트 프로그램을 구성하는 프로그램 모듈을 도시한다.

도 5는 어드레스 수집단계(S10)의 실행절차를 보다 구체적으로 도시한다.

도 6은 통신차단에 관한 룰 설정과 그에 따른 차단처리 절차를 도시한다.

도 7은 기 설정된 통신차단룰을 해제하는 절차를 도시한다.

도 8은 통신제어룰 DB에 설정된 룰에 따라 망내 장비들 간의 통신제어가 처리되는 절차를 도시한다.

도 9는 패킷의 검출과 그에 따른 어드레스 수집 절차에 대해 보다 구체적으로 나타낸다.

도 10은 검출된 패킷에 따른 통신제어처리 절차를 도시한다.

도 11은 도 10의 S184 단계의 'ARP 요청패킷의 검출에 따른 처리 루틴'을 보다 구체적으로 나타낸다.

도 12는 도 10의 S184 단계의 'ARP 응답패킷의 검출에 따른 처리 루틴'을 보다 구체적으로 나타낸다.

도 13은 프로토콜 레이어 패킷의 검출에 따른 처리 절차를 도시한다.

도 14는 도 13의 패킷포워딩 단계(S250)를 보다 구체적으로 나타낸 흐름도이다.

도 15는 ARP 응답패킷과 ARP 요청패킷의 검출에 따른 어드레스 DB의 관리단계(즉, 도 11의 S192단계와 도 12의 S212단계)의 절차를 도시한다.

도 16은 프로토콜 어드레스와 데이터링크 레이어 어드레스의 조합에 대해 설정된 통신제어룰을 검색하여 처리하는 것을 도시한다.

도 17과 18은 프로토콜 어드레스와 데이터링크 레이어 어드레스에 의한 통신제어룰을 검색하여 처리하는 것을 도시한다.

도 19는 망내 장비들의 어드레스를 검출하여 데이터베이스에 저장 관리하는 루틴을 도시한다.

** 도면의 주요부분에 대한 부호의 설명 **

10: 외부 장비 20: 인터넷

30: 라우터 40: 랜(LAN)

50: 레이어2 스위치

발명의 상세한 설명】

발명의 목적】

발명이 속하는 기술분야 및 그 분야의 종래기술】

본 발명은 하나의 네트워크 내부 장비들 간의 통신을 제어하는 기술에 관한 것로서, 보다 상세하게는 네트워크 내부 장비들에 대하여 통신 허용 또는 통제 등에 한 룰을 강제함으로써 네트워크 내부 장비들 간에 가상의 방화벽이 존재하는 것과은 환경을 구축할 수 있는 기술에 관한 것이다.

복잡 다양화 되어가는 네트워크 환경 하에서는 제한된 인적 자원을 통해 방대한트워크 자원을 효율적이고 통합적으로 관리하고 제어할 필요가 있다. 아이피nternet Protocol: IP) 어드레스, 미디어접근제어(Media Access Control: MAC) 어레스, 호스트 아이디(Host ID) 등과 같은 네트워크 자원은 이를 수동으로 관리하면]적 자원의 낭비와 업무능률의 저하가 초래된다. 또한 네트워크 사용자의 IP 도용 의해 기존 네트워크 장비의 IP와 충돌을 일으키는 장애가 발생되기도 한다.

일반적으로 회사나 공장 등은 업무의 효율성이나 생산성 향상을 위해 근거리 네워크(Local Area Network: LAN)를 이용한다. LAN에는 퍼스널컴퓨터(PC), 워크스테션, 로봇, 프린터, 서버 등과 같은 각종 장비들(이하 '망내 장비'라 함)이 수십 대서 수천 대씩 연결된다. 이들 망내 장비들 간의 통신이 아무런 제한 없이 허용하는

이 작업의 효율화와 편리함에 도움이 되는 측면도 있지만, 한편으로는 망내 장비 간의 무제한적인 통신 허용은 몇 가지 문제점을 남기도 한다. 즉, 망내 장비들 간 통신을 적절히 제한하지 않으면 필요하지 않는 데이터 패킷들이 LAN 상에 많이 돌아다니게 되고 이로 인해 네트워크 자원이 필요이상으로 사용되므로 네트워크 자원의 낭비가 초래된다. 또한, 네트워크 자원의 이용 내지 통신의 자유에 대한 통제가 없으면, 부정한 목적을 가진 네트워크 내부 이용자 간에 정보의 유출이나, 해킹, 크래킹 등의 행위가 아무런 제약을 받지 않고 이루어질 수 있는 취약점도 있다. 따라서 LAN 환경을 기반으로 하는 회사나 공장 등에서는 필요에 따라 LAN에 연결된 장비들 각각에 대하여 다른 장비들과의 통신을 적절히 제한할 필요가 있다. 이를 위해서는 네트워크 내부 자원들 간의 통신권능을 통제할 수 있는 수단이 필요하다.

통신을 통제하는 수단으로서 가장 널리 사용되는 것이 바로 방화벽 서버이다. 그런데 기존의 방화벽 서버는, 어떤 내부 네트워크(NET-IN)가 외부의 다른 네트워크(NET-OUT)와 연결되는 길목에 위치하여, 외부 네트워크(NET-OUT)에 연결된 외부의 어떤 장비와 내부 네트워크(NET-IN)의 망내 장비들 간의 통신을 통제하는 역할을 담당하였다.

그런데 기존의 방화벽 서버는 어떤 내부 네트워크(NET-IN)에 접근할 수 있는 출구 즉, 길목에 위치하여 통신을 통제하므로, 외부 네트워크(NET-OUT)와의 통신을 차단하는 등의 통제는 할 수 있어도 내부 네트워크(NET-IN) 내의 망내 장비들 간의 통신을 통제하는 것은 불가능하였다. 기존의 방화벽 서버는 또한 망내 장비들

의 통신을 통제하여야 할 필요성에 대해서는 인식을 결여하고 있다. 나아가, 내부 트워크(NET-IN)와 외부 네트워크(NET-OUT)의 길목에 위치한 통신통제 방식은, 통신 어룰(communication control rule)을 내부 네트워크(NET-IN)에 연결된 장비 전체에 률적으로 적용할 수밖에 없다. 그 결과 통신을 통제할 필요성이 없는 장비조차도 상 방화벽 서버를 거쳐 통신을 해야 된다. 따라서 방화벽 서버는 불필요한 처리 부을 많이 떠맡게 되고, 이로 인해 외부 네트워크와 내부 네트워크 간의 통신 속도가 저하되는 문제가 생긴다.

이러한 점들을 고려할 때, 기존의 방화벽서버에서는 처리할 수 없는, 특정 네트크 내부에 존재하는 망내 장비들 간의 통신을 네트워크 관리자가 효과적으로 제한 수 있는 수단이 절실히 요구된다.

발명이 이루고자 하는 기술적 과제】

본 발명은 특정 네트워크에 대하여 그 네트워크의 망내 장비들과 수평적인 레벨 동일 레벨)로 연결되어 필요에 따라서 상기 망내 장비들 간의 통신을 통제할 수 있 장치와 상기 네트워크 관리자가 이 장치를 이용하여 필요에 따라 상기 망내 장비 간의 통신을 통제할 수 있게 하는 방법을 제공하는 것을 그 목적으로 한다.

발명의 구성】

본 발명의 기본적인 개념은, 특정 네트워크의 관리자가 그 네트워크에 다른 장들과 동일레벨에 접속된 본 발명의 장치를 이용하여 통신제어룰을 설정하고, 설정 통신제어룰을 망내 장비들 간의 통신에 강제적으로 적용되도록 함으로써, 통제 대

인 장비들이 설정된 통신제어룰에 따라 망내 통신이 제한될 수 있도록 하는 것이다.

상기 목적을 달성하기 위한 본 발명의 일 측면에 따르면, 특정 네트워크 상의 비들 간의 통신을 제어하는 방법에 있어서, 상기 네트워크 상의 장비들과 동일 레에 위치한 통신제어장비를 이용하여, 통신차단 대상인 장비들에 대하여 데이터링크 이어 어드레스가 조작된 ARP 패킷을 제공하여 상기 차단대상 장비가 송신한 데이 패킷이 비정상적인 어드레스로 전송되도록 함으로써 상기 차단대상 장비들 간의 신을 차단하는 것을 특징으로 하는 통신제어방법이 제공된다.

상기 통신제어방법은, 바람직하게는, 통신차단의 대상이 아님에도 불구하고 통 차단상태에 있는 장비에 대해서는 상기 통신제어장치가 정상적인 어드레스 정보를 포하는 ARP패킷을 해당 장비에게 송신함으로써 그러한 통신차단상태를 해제 단계를 구비한다.

또한, 상기 통신제어방법은, 바람직하게는, 네트워크에 신규로 연결된 장비의 어드레스를 기존 장비들의 IP 어드레스와 비교하여 충돌이 있는 경우, 올바른 IP 드레스를 유니캐스트로 기존 장비들에게 전달하여 IP어드레스의 충돌을 해결하는 계를 더 구비한다.

상기 통신제어방법에 있어서, 상기 차단대상 장비들 간의 통신을 차단하기 위해 기 차단대상 장비의 일부 또는 전부의 데이터링크 레이어 어드레스를 상기 통신제 장비 데이터링크 레이어 어드레스 또는 상기 차단대상 장비의 것이 아닌 제3의 데 터링크 레이어 어드레스로 설정한다.

본 발명의 다른 측면에 따르면, 특정 네트워크 상의 장비들 간의 통신을 제어하 방법에 있어서, 통신제어장치가 네트워크 내에 존재하는 네트워크 레이어 어드레 (이더넷 아이피 어드레스)와 데이터링크 레이어 어드레스(MAC:media access ntrol)를 수집하는 단계; 네트워크 관리자가 수집된 어드레스에 대하여 원하는 통 제어를 하기 위해 설정한 통신제어룰을 DB에 저장하는 단계; 네트워크 내의 어떤 비가 망내 다른 장비와 통신을 하기 위해 송신한 어드레스결정프로토콜(ARP) 패킷 검출하는 단계; 통신제어룰 데이터베이스에 조회하여 검출된 ARP 패킷이 통신차 대상에 해당하는지를 판별하는 단계; 및 통신차단대상에 해당하는 경우 통신차단 위한 ARP패킷을 만들어 송신하는 단계를 구비하여 망내 장비들 간의 통신을 필요 따라 선택적으로 제어할 수 있는 것을 특징으로 하는 통신제어방법이 제공된다.

상기 통신제어방법에 있어서, 상기 어드레스 수집단계는 바람직하게는, 상기 네 워크의 어떤 장비가 망내 다른 장비와 통신하기 위해 브로드캐스팅 한 ARP 패킷을 기 통신제어장치가 수신하여 그 ARP 패킷에 내포된 네트워크 레이어 어드레스와 데 터링크 레이어 어드레스를 검출하는 방법 및/또는 네트워크 관리자가 직접 입력한 리대상 장비의 어드레스에 의거하여 상기 통신제어장치가 ARP 요청패킷을 송신하고 에 응하여 관리대상 장비가 보내온 ARP 응답패킷으로부터 네트워크 레이어 어드레 와 데이터링크 레이어 어드레스를 검출하는 방법에 따른다.

상기 통신제어방법에 있어서, 통신제어룰의 설정 대상은 네트워크 레이어 어드 스 상호간, 데이터링크 레이어 어드레스 상호간, 네트워크 레이어 어드레스와 데이 링크 레이어 어드레스 상호간의 통신이 될 수 있다. 나아가, 상기 통신제어룰의 설 대상은 네트워크 레이어 어드레스와 네트워크 레이어 어드레스 그룹 상호간, 데이

링크 레이어 어드레스와 데이터 링크 레이어 어드레스 그룹 상호간, 네트워크 레이
어드레스와 데이터 링크 레이어 어드레스 그룹 상호간, 데이터링크 레이어 어드레
와 네트워크 레이어 어드레스 그룹 상호간, 네트워크 레이어 어드레스 그룹과 데이
링크 레이어 어드레스 그룹 상호간의 통신을 더 포함할 수 있다.

상기 통신제어방법은, 바람직하게는, 통신제어장비가 보낸 ARP 요청패킷에 응하
망내 장비가 ARP 응답패킷을 보내오면 검출된 응답패킷에 포함되어 있는 송신측
드레스를 이용하여 관리툴을 검색하고, 검색결과 그 송신측 어드레스에 대하여 차
툴이 존재하면 송신측 프로토콜과 동일한 네트워크에 속하는 모든 프로토콜-데이터
크 레이어 어드레스DB(DB-3)에 대하여 차단패킷을 송신하는 단계를 더 구비할 수
다.

나아가, 상기 통신제어방법은, 네트워크 레이어 패킷의 검출에 따라 더 이상 통
차단의 대상이 아님에도 불구하고 여전히 통신차단상태로 되어 있는 장비에 대해
러한 통신차단상태의 해제를 위한 ARP패킷을 만들어 송신하는 단계를 더 구비하는
이 바람직하다. 더 나아가, 일정한 시간 마다 통신제어툴 데이터베이스에 따라 통
차단/통신차단해제를 위한 ARP요청 패킷을 송신하는 단계를 더 구비하는 것이 바람
하다.

더 나아가, 상기 통신제어방법은 수신측 데이터링크 레이어 어드레스가 차단 어
레스로서 패킷포워딩 툴이 존재하는 경우 수신된 프로토콜 레이어 패킷을 그 패킷
목적지 어드레스를 정상적인 데이터링크 레이어 어드레스로 하여 포워딩 하는 단
를 더 구비하는 것이 바람직하다.

상기 통신제어방법은 또한, 네트워크에 신규로 연결된 장비의 IP 어드레스를 기 장비들의 IP 어드레스와 비교하여 충돌이 있는 경우, 올바른 IP 어드레스를 유니스트로 기존 장비에 전달하여 IP어드레스의 충돌을 해결하는 단계를 더 구비하는 이 바람직하다.

한편, 본 발명의 목적을 달성하기 위한 본 발명의 또 다른 측면에 따르면, 어떤 트워크 상의 다른 장비들과 동일레벨에 위치하면서, 네트워크 관리자가 필요에 따 상기 다른 장비들 상호간의 통신을 차단할 수 있는 통신제어룰을 설정할 수 있는 경을 제공하고, 설정된 상기 통신제어룰을 데이터베이스에 저장 관리하면서, 통신 단 대상으로 설정된 장비들에 대하여 데이터링크 레이어 어드레스가 조작된 ARP 패을 제공하여 상기 차단대상 장비가 송신한 데이터 패킷이 비정상적인 어드레스로 송되도록 함으로써 상기 차단대상 장비들 간의 통신을 차단하는 것을 특징으로 하 통신제어장치가 제공된다.

상기 통신제어장치는 외부에서 어떤 특정 네트워크에 통신하고자 할 때 그 네트크와의 연결 길목이 되는 위치에 배치되어 통신을 통제하는 기존의 방화벽서버와는 르게, 그 네트워크에 대한 통신경로의 길목이 아닌 그 네트워크 내의 임의의 곳 컨대 다른 내부 장비들과 동일레벨에 위치하면서 통신제어가 필요한 장비에 대하여 P 테이블의 어드레스정보의 조작에 기반을 두는 통신제어룰을 강제적으로 적용함으써 그 장비들에 대해서만 선택적으로 통신을 제한할 수 있다. 이에 의해, 어떤 네워크에 있어서 그 네트워크의 내부 자원과 외부 네트워크의 자원 간의 불필요한 통을 차단하는 종래의 방화벽 서버의 기능을 물론이거니와, 그 네트워크의 내부 자원 간의 통신까지도 선별적으로 원하는 대로 제어하는 것이 가능하다. 따라서 네트워

자원을 절약을 도모할 수 있고, 나아가 내부 장비들 간의 인증되지 않은 정보의 출을 방지할 수 있다.

이하에서는 첨부한 도면을 참조하여 본 발명의 바람직한 일실시예에 관하여 상히 설명하기로 한다.

랜(Local Area Network: LAN)과 같은 특정의 네트워크에 연결된 자원들 간의 통은 ARP를 이용하여 이루어진다. ARP는 네트워크 레이어 어드레스(예컨대, 프로토콜 이어(L3) 어드레스)를 물리적 어드레스(예컨대, 데이터링크 레이어(L2) 어드레스) 대응시키기 위해 사용되는 프로토콜이다. 여기서 물리적어드레스라 함은 예컨대 더넷 또는 토큰링의 48비트(bits) 네트워크 카드 어드레스를 의미한다. ARP 패킷은 더넷 패킷 데이터 내의 한 부분으로 포함된다. 이더넷 패킷의 헤더는 목적지 이더 어드레스(48비트), 발신자 이더넷어드레스(48비트), 이더넷 프로토콜타입(16비트) 포함한다. 이 이더넷 패킷 헤더의 뒤에 ARP 패킷이 붙는다. 패킷이 LAN 상에서 이할 때에는 목적지 이더넷어드레스(예컨대 MAC 어드레스)로 전송된다. 참고로 ARP 킷은 다음과 같이 구성되어 있다.

【표 1】 ARP 패킷의 구성

구성요소	바이트 수	내용
드웨어타입	2	네트워크 계층에서 사용되는 하드웨어 형식을 나타낸다. 이더넷은 이 값은 1이다.
로토콜타입	2	네트워크 계층에서 사용되는 프로토콜을 나타낸다.
이터넷 레이어 드레스 길이	1	바이트안의 하드웨어 어드레스의 길이를 나타낸다. 이더넷인 경우에 값은 6이 된다.
로토콜 어드레스 이	1	바이트안의 프로토콜의 길이를 나타낸다. TCP/IP인 경우에 이 값은 4가 된다.
P 구분코드	2	이 필드는 ARP요구, ARP응답, RARP요구, RARP응답 같은 패킷의 명령들을 요사한다.
신 데이터링크 이어 어드레스	n	보낸 곳에서의 하드웨어 어드레스로 대부분의 경우 이더넷 어드레스가 된다.
신 프로토콜 드레스	m	보낸 곳의 인터넷 어드레스.
신 데이터링크 이어 어드레스	n	ARP요구가 발생했을 때, 이것이 도착지 하드웨어 어드레스가 된다. 응답은 도착지 기계의 하드웨어 어드레스와 인터넷 어드레스를 알려준다.
신 프로토콜 드레스	m	ARP요구가 발생했을 때, 이것이 도착지 인터넷 어드레스가 된다. 응답은 도착지 장비의 하드웨어 어드레스와 인터넷 어드레스를 알려준다.

예를 들어, IP 호스트 A가 IP 호스트 B에게 IP 패킷을 전송고자 할 때 IP 호스 B의 물리적 어드레스를 모르는 경우, IP 호스트 A는 ARP 프로토콜을 사용하여 목지인 IP 호스트 B의 IP 어드레스와 브로드캐스팅 물리적 어드레스 F:FF:FF:FF:FF:FF)를 가지는 ARP 패킷을 네트워크 상에 전송한다. IP 호스트 B는 신의 IP 어드레스가 목적지로 기록되어 있는 ARP 패킷을 수신하면 자신의 물리적 트워크 레이어 어드레스를 IP 호스트 A에게 응답한다. 이와 같은 방식으로 수집된 어드레스와 이에 해당하는 물리적 네트워크 레이어 어드레스 정보는 각 IP 호스트 ARP 캐시라 불리는 메모리에 테이블 형태(ARP TABLE)로 저장된 후, 다음 패킷 전시에 다시 사용된다. 랜(Local Area Network: LAN)과 같은 네트워크에 연결되어는 자원들끼리는 이와 같은 방식으로 내부 통신을 하게 된다.

ε 1은 본 발명에 따른 통신통제방법을 구현한 시스템 구성예이다. 다수의 장비들
Q-1, EQ-2, ... EQ-10)이 레이어2 스위치(50)를 통해 연결된 LAN(40) 환경에서, 본
명에 따른 통신제어장치(EQ-X)도 LAN(40)에 연결된 하나의 노드로서, 다른 장비들
Q-1, EQ-2, ... EQ-10)과 같은 레벨에 연결된다. 다만 원하는 장비에 대한 통신을
제하기 위한 방법으로서, ARP 테이블을 조작함으로써 LAN(40) 내부 장비들 간의 통
을 원하는 형태로 통제를 한다. LAN(40)은 라우터(30)를 경유하여 인터넷(20) 또는
나른 네트워크(예컨대 사내 다른 가상 LAN(VLAN)) 등에도 연결될 수 있다.

같은 네트워크 레이어 끼리 통신을 하기 위해서 ARP 프로토콜을 이용하여 데이
링크 레이어 어드레스를 구하고 데이터링크 레이어 어드레스를 이용하여 통신을 하
. 네트워크 레이어 어드레스와 데이터링크 레이어 어드레스를 ARP 테이블(네트워크
이어 어드레스-데이터링크 레이어 어드레스)로 관리하고 나중에 통신이 필요할 때
용한다.

본 발명의 기본적인 개념은, 특정 네트워크의 관리자가 그 네트워크에 다른 장
들과 등일레벨에 접속된 본 발명의 장치를 이용하여 통신제어룰을 설정하고, 설정
통신제어룰을 망내 장비들 간의 통신에 강제적으로 적용되도록 함으로써, 통제 대
인 장비들이 설정된 통신제어룰에 따라 망내 통신이 제한될 수 있도록 하는
이다.

하나의 네트워크 내에서 그 네트워크에 연결된 내부 장비들 간의 통신을 허용/
단/패킷포워딩 하는 등의 통신 제어를 하기 위해서는 각 장비의 ARP테이블을 외부
서 원하는 내용으로 만들거나 수정하는 등의 조작을 하고, 특정 네트워크 레이어
드레스와 통신이 필요할 때 그렇게 외부에서 조작된 ARP 테이블이 이용되도록 만들

있어야 한다. 또한 각 장비는 어느 때나 ARP테이블을 삭제하거나 새롭게 ARP요청 킷을 발생하여 데이터링크 레이어 어드레스를 구하려 하기 때문에 이에 대해서도 적절한 처리를 할 수 있어야 한다. 이 때 가장 중요한 것은 ARP패킷을 발생하여 ARP 테이블을 생성/수정하도록 만들 때 다른 장비들에는 영향을 주지 않고 원하는 장비에 적용이 되도록 하여야 한다. 즉, 제어가 필요하지 않은 다른 장비에 영향을 주지 않으면서 통제가 가능해야 한다. 이를 위해 통신제어대상 노드에 조작된 ARP 어드레스를 제공할 때 유니캐스트 전송방식을 이용한다. 또한 데이터링크 레이어 어드레스를 이용하여 통신을 차단을 하면 네트워크 레이어의 모든 것에 대해 차단이 되기 때문에 네트워크 레이어 패킷에 대해서는 필요한 경우에 포워딩할 수 있어야 한다. 통신이 필요한 네트워크 레이어 패킷에 대해서는 본 발명의 통신제어장치가 포워딩을 하여 통신이 가능하도록 중계해줄 수 있어야 한다.

이와 같은 통신통제방식이 가능함을 이해하기 위해선, LAN 상에서 망내 장비들의 통신이 어떻게 이루어지는지에 대한 이해가 선행될 필요가 있다. 이와 관련하여 망내 장비들 간의 통신 메커니즘을 예시적으로 설명함으로써 통신제어장치 EQ-X가 어떠한 원리로 망내 장비들 간의 통신을 통제할 수 있는지에 관한 이해를 돕기로 한다.

예컨대, 현재 LAN(40)에 연결된 망내 장비가 EQ-1, EQ-2, EQ-3이고 통신제어장치 EQ-X가 이들 장비와 같은 레벨에 연결되어 있는 환경과, 모든 장비에는 ARP

이블이 처음에는 비어 있다는 조건을 가정하자. 이들 장비 EQ-1, EQ-2, EQ-3, EQ-X IP어드레스와 MAC 어드레스는 각각 NET-1(MAC-1), NET-2(MAC-2), NET-3(MAC-3), T-X(Block) 이라고 가정한다. 여기서 수신측 어드레스와 송신측 어드레스는 'IP어레스(MAC 어드레스)'의 형식으로 표현되었다. 그리고 망내 장비들 간에 통신을 위 다음과 같은 ARP 요청 패킷들이 송신되었다고 가정하자. 단 ARP 패킷은 브로드캐트(FF:FF:FF:FF:FF:FF)가 아닌 유니캐스트 방식으로 송신했음을 전제한다.

1) 과정 1 : 목적지 MAC이 MAC-1이고 수신측 어드레스와 송신측 어드레스가 각 NET-1(Null)과 NET-2(Block)인 요청패킷(요청패킷1)이 송신된다. 참고로, 요청패 1은 장비 EQ-2가 장비 EQ-1과 통신을 하기 위한 ARP 요청패킷으로 볼 수 있다. 이 청패킷1의 목적지 MAC 어드레스(즉, MAC-1)와 일치하는 장비 EQ-1이 이 요청패킷1 수신한다. 그리고 장비 EQ-1은 장비 EQ-2의 MAC 어드레스가 Block인 것으로 인식다. 이러한 인식에 의해, 장비 EQ-1이 장비 EQ-2에 보내는 패킷은 실제로는 MAC 어레스가 Block인 통신제어장치 EQ-X가 수신하게 된다.

2) 과정 2 : 목적지 MAC은 MAC-2이고 수신측 어드레스와 송신측 어드레스를 각 NET-2(MAC-2)와 NET-1(Block)로 가지는 요청패킷(요청패킷2)이 송신된다. 참고로, 요청패킷1은 MAC 어드레스가 MAC-2인 장비 EQ-2가 수신하게 된다. 장비 EQ-2는 장 EQ-1의 MAC 어드레스가 Block인 것으로 인식한다. 이러한 인식에 의해, 장비 EQ-2 장비 EQ-1에 보내는 패킷은 실제로는 MAC 어드레스가 Block인 통신제어장치 EQ-X 수신하게 된다.

3) 과정 3 : 목적지 MAC은 MAC-3이고 수신측 어드레스와 송신측 어드레스를
T-3(Null)과 NET-1(MAC-1)로 가지는 요청패킷(요청패킷3)이 송신된다. 이는 장비
-1이 장비 EQ-3과 통신하기 위한 ARP 요청패킷으로 볼 수 있다.

4) 과정 4 : 목적지 MAC은 MAC-3이고 수신측 어드레스와 송신측 어드레스를 각
NET-3(Null)과 NET-2(MAC-2)로 가지는 요청패킷(요청패킷4)이 송신된다.

이 송신과정을 표로 정리하면 아래와 같다.

[표 2]

신과정	패킷	목적지 MAC	수신어드레스	송신어드레스
과정 1	요청패킷 1	MAC-1	NET-1(null)	NET-2(BLOCK)
과정 2	요청패킷 2	MAC-1	NET-2(null)	NET-1(BLOCK)
과정 3	요청패킷 3	MAC-3	NET-3(null)	NET-1(MAC-1)
과정 4	요청패킷 4	MAC-3	NET-3(null)	NET-2(MAC-2)

이러한 송신과정을 통해 송신된 4개의 요청패킷을 수신한 장비들은 다음과 같이
응답패킷의 송신으로 답한다.

5) 과정5 :'요청패킷1'을 수신한 장비 EQ-1 (NET-1, MAC-1)은 NET-1(MAC-1)을
신측으로 하고, NET-2(Block)를 수신측으로 하며, 목적지 MAC을 BLOCK으로 하는
P 응답패킷(응답패킷1)을 보내고, 자신이 관리하는 ARP 테이블에는 NET-2에 대한
C 어드레스를 BLOCK으로 기록하여 신규 생성한다.

6) 과정6 :'요청패킷2'를 수신한 EQ-2 (NET-2, MAC-2)는 NET-2(MAC-2)를 송신측
로 하고 수신측을 NET-1(BLOCK)로 하며, 목적지 MAC을 BLOCK으로 하는 ARP 응답패
(응답패킷2)을 보내고, 자신의 ARP 테이블에는 NET-1에 대한 MAC 어드레스를 BLOCK
로 신규 생성한다.

7) 과정7 : '요청패킷3'을 수신한 EQ-3 (NET-3, MAC-3)은 NET-3(MAC-3)을 송신측로 하고, NET-1(MAC-1)을 수신측으로 하며, 목적지MAC을 NET-1로 하는 ARP 응답패(응답패킷3)을 보내고, 자신의 ARP 테이블에서 NET-1에 대해서 MAC-1로 신규 생성다.

8) 과정 8 : '요청패킷4'를 수신한 EQ-3 (NET-3, MAC-3)은 NET-3(MAC-3)을 송신으로 하고 수신측을 NET-2(MAC-2)로 하며, 목적지MAC을 NET-2로 하는 ARP답패킷(응답패킷4)을 보내고, 자신의 ARP 테이블에서 NET-2에 대해서 MAC-2로 신규§성한다.

위 응답과정을 정리하면 다음과 같다.

[표 3]

응답 과정	패킷/ 응답장비	응답 내용	ARP 테이블
정 5	응답패킷 1 / EQ-1	송신측 어드레스: NET-1(MAC-1) 수신측 어드레스: NET-2(BLOCK) 목적지 MAC : BLOCK	NET-2에 대한 MAC어드레스를 BLOCK으로 생성
정 6	응답패킷 2 / EQ-2	송신측 어드레스: NET-2(MAC-2) 수신측 어드레스: NET-1(BLOCK) 목적지 MAC : BLOCK	NET-1에 대한 MAC어드레스를 BLOCK으로 생성
정 7	응답패킷 3 / EQ-3	송신측 어드레스: NET-3(MAC-3) 수신측 어드레스: NET-1(MAC-1) 목적지 MAC : MAC-1	NET-1에 대한 MAC어드레스를 MAC-1로 생성
정 8	응답패킷 4 / EQ-3	송신측 어드레스: NET-3과 MAC-3 수신측 어드레스 : NET-2(MAC-2) 목적지 MAC : MAC-2	NET-2에 대한 MAC 어드레스를 MAC-2로 생성

다음으로, 위와 같은 4 개의 응답패킷을 수신한 각 장비 내에서는 다음과 같은리가 이루어진다.

9) 과정 9 : '응답패킷1'을 수신한 통신제어장치 EQ-X는 ARP 테이블에 IP어드레 NET-1에 대해서 MAC 어드레스를 MAC-1로 신규 생성한다. 왜냐하면 응답패킷1이 송측을 MAC-1로 하여 송신하였기 때문이다.

10) 과정 10 : '응답패킷2'를 수신한 통신제어장치 EQ-X는 ARP 테이블에 NET-2 대해서 MAC-2를 신규 생성한다.

11) 과정 11 : '응답패킷3'을 수신한 장비 EQ-1은 ARP 테이블에 NET-3에 대해서 C-3을 신규 생성한다.

12) 과정 12 : '응답패킷4'를 수신한 장비 EQ-2는 ARP 테이블에 IP어드레스 T-3에 대해서 MAC 어드레스 MAC-3을 신규 생성한다.

이러한 처리 내용을 정리하면 다음과 같다.

[표 4]

과정	장비	수신한 응답패킷	ARP 테이블에 대한 처리 내용
과정9	EQ-X	응답패킷1	NET-1에 대해서 MAC-1을 신규 생성
과정10	EQ-X	응답패킷2	NET-2에 대해서 MAC-2를 신규 생성
과정11	EQ-1	응답패킷3	NET-3에 대해서 MAC-3을 신규 생성
과정12	EQ-2	응답패킷4	NET-3에 대해서 MAC-3을 신규 생성

위와 같은 과정이 끝난 후의 각 장비에 유지되고 있는 ARP 테이블을 살펴보면 음과 같은 내용으로 변경이 있게 된다.

장비 EQ-1이 유지하고 있는 엔트리는 NET-2(BLOCK)와 NET-3(MAC-3)이고(테이블 (과정5. 과정11).

장비 EQ-2가 유지하고 있는 엔트리는 NET-1(BLOCK)과 NET-3(MAC-3)이고(테이블
(과정6, 과정12).

장비 EQ-3이 유지하고 있는 엔트리는 NET-1(MAC-1)과 NET-2(MAC-2)이고(테이블
(과정7, 과정8).

장비 EQ-X가 유지하고 있는 엔트리는 NET-1(MAC-1)과 NET-2(MAC-2)이다(테이블
(과정9, 과정10).

이를 표로 정리하면 다음과 같다.

[표 5]

-비	ARP테이블	엔트리 1	엔트리 2	관여 과정
)-1	테이블 1	NET-2(BLOCK)	NET-3(MAC-3)	과정5, 과정11
)-2	테이블 2	NET-1(BLOCK)	NET-3(MAC-3)	과정6, 과정12
)-3	테이블 3	NET-1(MAC-1)	NET-2(MAC-2)	과정7, 과정8
)-x	테이블 4	NET-1(MAC-1)	NET-2(MAC-2)	과정9, 과정10

장비 EQ-1과 EQ-3의 ARP 테이블인 테이블1과 테이블3의 경우 동일한 장비 EQ-2 어드레스인 NET-2에 대해 MAC어드레스인 BLOCK과 MAC-2를 가지고 있기 때문에, 장 EQ-1과 EQ-3이 장비 EQ-2에게 패킷을 보내려할 때 송신 패킷의 목적지가 다르게 다. 그리고 장비 EQ-2와 EQ-3의 ARP 테이블인 테이블2와 테이블3을 보면, 동일한 비 EQ-1에 대해 서로 다른 MAC 어드레스인 BLOCK과 MAC-1을 가지고 있기 때문에 장 EQ-2와 EQ-3이 장비 EQ-1에게 패킷을 보내려할 때 보내지는 패킷은 목적지가 다르 된다. 따라서 장비 EQ-1과 EQ-3 간의 통신과 장비 EQ-2와 장비 EQ-3 간의 통신은 상적으로 이루어질 수 있지만, 장비 EQ-1과 장비 EQ-2 간의 통신은 통신제어장치 -X에 설정되어 있는 통신제어툴에 따라 가능한지 여부가 결정이 된다.

위에서 설명한 망내 장비들 간의 통신 메커니즘에 입각할 때, ARP 테이블의 어레스를 적절히 조작하면 망내 장비들 간의 통신을 원하는 형태로 통제할 수 있게을 알 수 있다. 이러한 이해에 기초하여 본 발명이 채용하는 방법은 통신제어장치 -X가 망내 장비들(EQ-1, EQ-2, EQ-3, ...) 중 통신의 차단 또는 패킷포워딩 등과은 통신통제의 대상 장비에 대해 통신 통제를 위해 의도적으로 조작된 어드레스 정를 내포하고 있는 ARP패킷을 만들어 송신하는 것이다. 통신제어를이 장비 EQ-1과비 EQ-2 간의 통신을 차단하는 것으로 설정된 경우를 가정하자. 통신제어장치 EQ-X 그 통신제어를에 따라서 장비 EQ-1과 장비 EQ-2 간의 통신을 차단하기 위하여 통제어장치 EQ-X가 이들 두 장비에 ARP 어드레스를 조작한다. 즉, 통신제어장치 EQ-X 장비 EQ-1에게는 장비 EQ-2의 ARP 어드레스를 N2-MX로 조작하여 제공함과 동시에비 EQ-2에게는 장비 EQ-1의 ARP 어드레스를 N1-MX로 조작하여 제공한다. 이렇게 조된 ARP 어드레스를 유니캐스트로 수신한 두 장비 EQ-1과 EQ-2는 자신의 ARP 테이블 그 조작된 어드레스를 반영하고, 이후의 통신은 갱신된 ARP 테이블 엔트리에 기초여 이루어진다. 이를 정리하면 아래 표 6과 같다.

[표 6]

\RP 테이블	EQ-1(N1-M1)	EQ-2(N2-M2)	EQ-3(N3-M3)
정상 상태	N2-M2, N3-M3	N1-M1, N3-M3	N1-M1, N2-M2
조작된 상태	N2-MX, N3-M3	N1-MX, N3-M3	

이에 의해, 제1장비와 제2장비 각각은 통신제어장치 EQ-X가 마치 통신상대방인 2장비와 제1장비인양 인식하게 된다. 따라서 두 장비 EQ-1과 EQ-2가 송신하는 패킷 MAC 어드레스가 MX인 통신제어장치 EQ-X로 전달된다. 즉, 망내 어떤 장비와 통신 하고자 하는 특정 장비가 송신한 패킷은 관련 장비들의 ARP 테이블을 조작함으로

항상 통신제어장치 EQ-X(또는 제3의 어드레스)에게 전해지도록 할 수 있다. 통신제어장치 EQ-X는 두 장비로부터 수신한 그 패킷을 무시해버리면 두 장비 간의 통신은 차단되고, 이에 의해 통신제어장치가 망내 장비들 간의 통신을 그들 장비의 의지와 상관없이 통제할 수 있게 됨을 알 수 있을 것이다.

또한, 네트워크에 신규로 연결된 장비의 IP 어드레스가 기존 망내 장비와 IP 충돌을 일으키는 경우가 발생할 수 있는데, 통신제어장치는 이러한 IP 어드레스의 충돌을 자동으로 해결해 줄 수 있다. 즉, MAC 어드레스가 MAC-9인 신규 장비 EQ-9가 IP 어드레스를 NET-1로 정하여 통신을 위한 브로드캐스팅을 하게 되면 이를 통신제어장치 EQ-X가 검출하게 된다. 그런 다음 신규 장비 EQ-9의 어드레스를 올바른 'IP어드레스-MAC 어드레스' 정보를 정리하고 있는 통신통제를 DB에 조회하여 과연 신규 장비의 IP어드레스가 올바른지를 판단한다. 이러한 판단결과 신규 장비의 IP어드레스가 기존의 IP어드레스와 충돌을 일으키는 것으로 판단되면, 올바른 IP 어드레스를 유니캐스트로 기존 장비들에 전달하여 IP어드레스의 충돌을 해결한다.

나아가, 통신제어장치 EQ-X는 더 이상 통신통제의 대상이 아님에도 불구하고 여전히 통신통제상태로 유지되고 있는 장비에 대해서는 그러한 통신통제상태를 해제하여 정상적인 통신이 이루어지도록 해줄 수 있어야 한다. 이러한 해제를 위해 통신제어장치 EQ-X는 정상적인 어드레스정보를 내포하는 ARP패킷을 만들어 해당 장비에게 전송한다. 특히, ARP 요청패킷을 보내는 방법에 있어서 가장 중요한 것은 브로드캐스트 패킷으로 보내는 것이 아니라 필요한 장비들 각각에게 유니캐스트 패킷으로 송신하여, 그 유니캐스트 패킷을 수신한 장비의 ARP 테이블에 원하는 엔트리(네트워크 레이어 어드레스, 데이터링크 레이어 어드레스)를 유지하도록 하는 것이다.

통신제어를을 설정하는 방법은 여러 가지가 가능하다. 통신제어장치 EQ-X가 망 두 장비 EQ-1과 EQ-2 간의 통신을 통제하는 를을 설정하는 경우를 예로 하여 설명다.

첫 번째 방법은 도 3의 (a)에 도시된 바와 같이, 장비 EQ-1과 장비 EQ-2가 서로 }대방에게 보내고자 하는 모든 패킷을 통신제어장치 EQ-X가 항상 반도득 설정하여 신제어장치 EQ-X가 이들 두 장비 간의 통신권능을 조회하여 통신을 허용하거나 또 차단하는 조치를 취하는 방법이다.

두 번째 방법은 도 3의 (b)에 도시된 바와 같이, 장비 EQ-1이 장비 EQ-2에게 패을 송신하는 경우에는 통신제어장치 EQ-X를 거치지 않고 직접 전송되도득 하되, 장 EQ-2에서 장비 EQ-1로 전송되는 패킷은 반드시 통신제어장치 EQ-X에 먼저 전달되득 설정하는 방법이다.

세 번째 방법은 도의 (c)에 도시된 바와 같이 위 두 번째 방법과는 반대로, 장 EQ-1에서 장비 EQ-2로 송신되는 패킷은 반드시 통신제어장치 EQ-X에 먼저 전달되득 하고 장비 EQ-2에서 장비 EQ-1로 송신되는 패킷을 직접 전달되도득 설정하는 방이다.

이와 같은 개념에 기초한 망내 장비들 간의 통신제어는 소프트웨어적으로 실현 수 있으며, 이를 위한 수단은 소프트웨어와 이를 내장한 컴퓨터(즉, 통신제어장치 Q-X)가 된다. 본 발명의 구현을 위해 필요한 프로그램은 크게 세 부분 즉, 서버 프그램, 에이전트 프로그램, 그리고 클라이언트 프로그램이 필요하다. 이들 세 프로램은 같은 장치, 즉 통신제어장치 EQ-X에 전부 위치할 수도 있고 다른 장치에 위치 수도 있다. 에이전트 프로그램은 서버 프로그램을 통하여 설정된 통신제어를 및

집한 어드레스자료를 이용하여 특정 장비 간의 통신제어를 실제로 담당하는 프로그
으로서, 다수 개로 구성될 수 있다. 서버 프로그램은 여러 에이전트 프로그램들을
합 관리하고 사용자로부터의 에이전트 프로그램에 대한 명령을 전달하는 역할을 담
하고, 에이전트 프로그램으로부터 수집된 자료를 통합 관리하는 프로그램이다. 클
이언트 프로그램은 사용자를 위한 인터페이스 역할을 담당하는 프로그램으로서, 관
자 컴퓨터에 설치되는 전용 클라이언트 프로그램이거나 또는 웹방식으로 사용할 수
는 웹용 프로그램이다.

특히 에이전트 프로그램은 본 발명에 따른 통신제어를 실현하는 데 핵심적인 역
을 하는 기능을 갖고 있다. 이 프로그램은 여러 개의 이더넷 인터페이스를 보유하
여러 네트워크를 관리할 수 있고, 또한 802.1Q의 VLAN을 이용한 방식을 취함으로
하나의 이더넷 인터페이스를 이용하여 여러 네트워크를 관리 및 통제를 할 수 있
기능도 가진다. 에이전트 프로그램은 도 4에 도시된 바와 같은 구조를 갖는 여러
의 모듈로 구성된다. 에이전트 프로그램을 구성하는 모듈의 종류와 각각의 주요 기
은 다음과 같다.

[표 7]

모듈 종류	주요 기능
과를 위한 통신모듈	서버를 통한 통신제어들의 관리를 위한 수신, 수집된 자료와 이벤트의 송신
단/해제 관리 모듈	수신된 패킷 또는 관리자의 명령에 의해 통신 차단/해제를 실행
단모듈	ARP 패킷을 이용하여 통신차단을 위한 ARP 패킷을 송신
제모듈	ARP 패킷을 이용하여 통신차단상태를 해제하기 위한 ARP 패킷을 송신함
드레스 및 차단를 DB 리모듈	여러 가지 어드레스 및 차단를 DB들을 관리함
킷 차단 모듈	프로토콜 레이어에서의 통신차단 패킷을 송신 함
킷포워딩 모듈	프로토콜 레이어에서 ARP에 의해 차단된 것 중 포워딩이 필요한 패킷을 포워딩 함
킷 검출 모듈	네트워크인터페이스로부터의 패킷 수신하여 네트워크 카드로부터 ARP 패킷을 검출함

에이전트 프로그램은 신속한 처리를 위하여 모든 DB를 메모리에 HASH 및 데이터 크드 리스트를 이용하여 관리한다. 관리하는 DB의 종류는 다음과 같다. 이들 DB를 리하는 것이 바로 어드레스 및 차단를 DB 관리모듈이다.

【표 8】

DB 명	관리 내용
로토콜어드레스DB (DB-1)	프로토콜어드레스, 차단여부, 차단기간, 고정여부(프로토콜어드레스를 데이터링크 레이어 어드레스에)
이터링크-MAC어드레스 DB B-2)	데이터링크 레이어 어드레스, 차단여부, 차단기간, 고정여부(데이터링크 레이어 어드레스를 프로토콜 어드레스에)
로토콜-데이터링크 레이어 드레스DB(DB-3)	프로토콜/데이터링크 레이어 어드레스, 고정여부, 최근 활동 시간
로토콜어드레스그룹 DB B-4)	프로토콜어드레스 그룹, 그룹 내 장비끼리 통신여부
이터링크 레이어 어드레스 룹 DB (DB-5)	데이터링크 레이어 어드레스 그룹, 그룹 내 장비끼리 통신여부
EM단위 룹DB (DB-6)	단위의 프로토콜(데이터링크)어드레스에 대하여 프로토콜(데이터링크)어드레스 및 프로토콜(데이터링크)그룹과의 차단/포워딩 룹 설정 관리
룹 간의 룹DB (DB-7)	프로토콜/데이터링크 레이어 어드레스그룹과 프로토콜/데이터링크 레이어 어드레스그룹사이의 차단/포워딩룹 설정 관리
리대상설정DB (DB-8)	관리할 프로토콜 어드레스 범위 설정

다음으로, 도 2는 LAN(40)에 연결된 망내 장비들에 대한 통신을 제어하는 본 발에 따른 방법을 개략적으로 도시한다.

LAN(40)에 연결된 망내 장비들(EQ-1, EQ-2, ..., EQ-10) 간의 통신을 제어하기 해, 우선적으로 수행해야 할 절차는 LAN(40) 내에 존재하는 네트워크 레이어 어드스와 데이터링크 레이어 어드레스를 수집하는 것이다(S10 단계). 네트워크 레이어 드레스의 대표적인 예는 IP어드레스이고, 데이터링크 레이어 어드레스의 대표적인 는 MAC 어드레스이다. 도 5는 어드레스 수집단계(S10)의 실행절차를 보다 구체적으 도시한다. 어드레스의 수집은 크게 두 가지 방식으로 이루어진다. 하나는 새로운 비가 LAN(40)에 추가되어 망내 다른 장비와 통신하고자 할 때, ARP 패킷을 브로드스팅 하여 다른 장비의 응답을 요청하는데, 통신제어장치가 그 과정에서 발생되는 P 패킷을 접수하여 그 새로운 장비의 어드레스를 수집하는 경우이다. 구체적으로, N(40) 내부의 어떤 장비가 망내 다른 장비와 통신을 하기 위해 ARP 패킷을 브로드스팅 할 때(S100), 통신제어장치 EQ-X가 그 ARP 패킷을 수신하여 그 속의 네트워크 이어 어드레스와 데이터링크 레이어 어드레스를 검출(S102)하는 방식이다. 다른 나는 네트워크 관리자가 관리대상 장비의 어드레스를 직접 입력하면 그 입력 어드스로부터 수집하는 방식이다. 즉, 네트워크 관리자가 통신제어를 위한 관리대상을 리대상 DB에 설정하면(S106), 그 설정 내용은 관리대상 DB에 저장되고(S108), 나아 통신제어장치는 관리대상 DB에 설정되어 있는 관리대상 장비에 대하여 ARP 패킷을 캐스트 방식으로 송신하고(S110), 이에 응답하여 관리대상 장비가 ARP 패킷을 신하면(S112), 통신제어장치는 그 ARP 패킷을 수신하여 그 속에 내포된 네트워크

이어 어드레스와 데이터링크 레이어 어드레스를 검출(S102)하는 방식이다. 어느 방
에 의해서건, 수집된 어드레스는 어드레스 DB에 저장, 관리된다.

다음으로 수집된 어드레스에 기초하여 네트워크 관리자가 네트워크 레이어 어드
스 및 데이터링크 레이어 어드레스에 대해서 통신제어룰을 설정한다(S20). 그리고
신제어룰이 설정되면, 통신제어장치(EQ-X)는 그 설정된 통신제어룰에 따라서 망내
비들 간의 통신을 차단, 해제 또는 패킷포워딩 등과 같은 처리를 한다(S30). 통신
단에 관한 룰 설정과 그에 따른 차단처리 절차를 도시한 도 6을 참조하여 이에 관
여 보다 구체적으로 설명하기로 한다.

도 6에서, 네트워크 관리자는 통신을 제어해야 할 망내 장비들에 대하여 통신제
룰을 설정한다. 통신제어룰의 설정은 다음과 같은 단계에 의해 수행된다. 첫째로,
트워크 내에 존재하는 네트워크 레이어 어드레스(이더넷 아이피 어드레스)와 데이
링크 레이어 어드레스(MAC 어드레스)에 관한 수집된 자료 및 수작업으로 입력한 자
를 바탕으로 네트워크 레이어 어드레스 그룹, 데이터링크 레이어 어드레스 그룹을
성한다. 다만, 네트워크 레이어 어드레스 그룹과 데이터링크 레이어 어드레스 그룹
공통성이 있는 어드레스 자원들을 같은 그룹으로 묶어서 관리하는 것이 편리한 경
에 이용하면 되므로, 반드시 채용해야 하는 필수적인 단계는 아니다. 둘째로, 각각
네트워크 레이어 어드레스, 데이터링크 레이어 어드레스, 네트워크 레이어 어드레
그룹, 데이터링크 레이어 어드레스 그룹에 대해 원천적으로 통신을 차단할 것인지
아니면 원천적인 통신 차단은 하지는 않을 것인지에 관한 설정을 한다. 즉, 통신의
천적인 허용/차단 여부 설정한다. 셋째로, 전체 네트워크 레이어 어드레스 각각에
해서 각 네트워크 레이어 어드레스와 다른 네트워크 레

어 어드레스, 데이터링크 레이어 어드레스, 네트워크 레이어 어드레스 그룹, 데이
링크 레이어 어드레스 그룹 간의 통신을 허용할 것인지 혹은 차단할 것인지 여부를
설정한다. 넷째로, 전체 데이터링크 레이어 어드레스 각각에 대해서 각 데이터링크
이어 어드레스와 다른 네트워크 레이어 어드레스, 데이터링크 레이어 어드레스, 네
워크 레이어 어드레스 그룹, 데이터링크 레이어 어드레스 그룹 간의 통신 허용할
인지 혹은 차단할 것인지 여부를 설정한다. 다섯째, 전체 네트워크 레이어 어드레
그룹에 대해서 각 네트워크 레이어 어드레스 그룹과 다른 네트워크 레이어 어드레
그룹, 데이터링크 레이어 어드레스 그룹 간의 통신 차단 여부 설정한다. 여섯째,
체 데이터링크 레이어 어드레스 그룹에 대해서 각 데이터링크 레이어 어드레스 그
과 네트워크 레이어 어드레스 그룹, 다른 데이터링크 레이어 어드레스 그룹 간의
신 차단 여부 설정한다. 도 3에 도시된 것과 같이, 통신차단룰을 설정하는 경우에
킷경로에 대해 방향성을 설정할 수도 있다.

이와 같은 통신제어룰의 설정은 네트워크 관리자가 통신제어장치 EQ-X를 이용하
직접 수동으로 입력하며, 입력된 통신제어룰은 통신제어룰 DB에 저장 관리되며,
시에 관리를 위한 용도로 통신제어룰을 설정한 시간 등을 어드레스 DB에 기록해둔
(S123, S124, S125). 통신제어룰의 설정 대상은 상기 통신제어룰의 설정 대상은 네
워크 레이어 어드레스 상호간, 데이터링크 레이어 어드레스 상호간, 네트워크 레이
어드레스와 데이터링크 레이어 어드레스 상호간의 통신이다. 나아가, 네트워크 레
어 어드레스와 데이터링크 레이어 어드레스에 그룹 개념을 도입하는 경우, 네트워
레이어 어드레스와 네트워크 레이어 어드레스 그룹 상호간,

이터링크 레이어 어드레스와 데이터 링크 레이어 어드레스 그룹 상호간, 네트워크
이어 어드레스와 데이터 링크 레이어 어드레스 그룹 상호간, 데이터링크 레이어 어
레스와 네트워크 레이어 어드레스 그룹 상호간, 네트워크 레이어 어드레스 그룹과
이터 링크 레이어 어드레스 그룹 상호간의 통신도 통신제어툴의 설정 대상이 된다.
신제어의 내용은 통신의 차단, 패킷포워딩, 차단의 해제, 허용 등과 같은 것이 될
있다. 예컨대, 망내 장비들의 네트워크 레이어 어드레스와 데이터링크 레이어 어
레스가 각각 NET-i (단, i=0, 1, 2, ..)와 MAC-j (단, j=0, 1, 2, ...)라 하자. 망
장비들의 관리 등의 필요에 따라 여러 개의 네트워크 레이어 어드레스 또는 여러
의 데이터링크 레이어 어드레스를 하나의 그룹으로 묶어서 관리하는 경우가 있다.
처럼 어드레스에 대하여 그룹개념을 도입하여 관리하는 경우, 네트워크 레이어 어
레스 그룹과 데이터링크 레이어 어드레스 그룹을 각각 NETG-m (단, m=0, 1, 2,...)
MACG-n (단, n=0, 1, 2,...)라 하자. 어드레스 그룹은 관리의 필요나 편의성을 고
하여 만들어지는 것이므로, 어떤 장비의 어드레스가 여러 그룹에 속할 수도 있고
느 그룹에도 전혀 속하지 않을 수도 있을 것이다. 예컨대 네트워크 레이어 어드레
가 NET-1인 장비에 대하여 통신제어툴은 다음과 같이 설정할 수 있다. 다른 네트워
레이어 어드레스나 데이터링크 레이어 어드레스, 그리고 이들 어드레스들의 각 그
에 대하여도 같은 방식으로 통신제어툴을 설정할 수 있다.

[표 9]

송신대상 어드레스	통신 상대측 어드레스	통신제어툴
NET-1	NET-2	차단
NET-1	NET-3	허용
NET-1	NET-4	허용
NET-1	NET-5	포워딩
...	.....	...
NET-1	NETG-1	차단
NET-1	NETG-2	허용
...	....	...
NET-1	MAC-1	허용
NET-1	MAC-2	차단
NET-1	MAC-3	포워딩
...	....	...
NET-1	MACG-1	차단
NET-1	MACG-2	허용
...	....	...

이상의 과정을 통해 망내 장비들에 대한 어드레스의 수집과 그 수집된 어드레스 대한 통신통제툴이 설정되면, 설정된 통신제어툴에 기초하여 망내 장비들 간의 통을 통제할 수 있는 조건이 마련된다. 이런 조건하에서 네트워크 내의 특정 장비 -i가 망내 다른 장비 EQ-j와 통신을 하기 위해 ARP 패킷을 브로드캐스팅 방식으로 신을 하면(S120), 통신제어장치 EQ-X도 그 ARP 패킷을 수신하게 되며, 그 ARP 패킷에 내포된 네트워크 레이어 어드레스와 데이터링크 레이어 어드레스를 검출한다. 신제어장치 EQ-X는 검출된 어드레스들을 통신제어툴 DB에 미리 등록되어 있는 정보 비교를 하여 검출된 어드레스가 통신차단의 대상인지를 판별한다. 통신차단의 대인 경우, 통신제어장치는 통신차단을 위한 조작된 ARP 패킷을 망내 모든 장비들에 유니캐스트 방식으로 송신한다. 조작된 ARP 패킷에는 통신의 주체가 되는 장비 -i와 EQ-j의 MAC 어드레스가 아닌, 통신제어장치 EQ-X 또는 제3의 장비의 MAC 어드스가 설정되어 있다. 그 결과 장비 EQ-i와 장비 EQ-j 간에 전송하고자 하는 패킷은

통신제어장치 EQ-X (또는 제3의 장비)에 먼저 전달된 후 통신 상대방으로 전달되지 고 무시되도록 처리함으로써 위 두 장비들 간의 통신이 차단된다.

통신차단의 대상이었던 어드레스가 어떤 사정에 의해 앞으로는 자유로운 통신이 장되도록 할 필요가 있을 수 있다. 이 경우 네트워크 관리자는 통신차단으로 설정 물이 해제되도록 재설정할 수 있고, 그에 의해 통신차단이 해제되는 처리가 이루 질 필요가 있다. 이러한 처리가 도 7에 도시되어 있다. 관리자는 통신제어장치 Q-X)를 이용하여 통신차단을 해제하기 위한 룰을 설정한다. 설정된 해제룰 역시 통 제어룰 DB에 기록되고, 그러한 해제룰의 설정시간 등이 어드레스 DB에 관리목적으 기록된다(S144, S142, S146). 한편, 네트워크 내의 특정 장비 EQ-i가 다른 장비 -j와 통신하기 위해 네트워크 레이어 패킷(예컨대 IP 패킷)을 브로드캐스팅 방식으 송신하면(S130), 통신제어장치 EQ-X는 그 패킷을 수신하여 그 속에 내포된 네트워 레이어 패킷을 검출한다(S132). 참고로 어드레스 통신차단의 해제는 항상 레이어 L3) 패킷을 이용하여 이루어진다. 그런 다음, 통신차단의 대상인 경우에만 통신차 의 해제를 할 사정이 있기 때문에, 검출된 패킷에 포함된 데이터링크 레이어 어드 스가 차단 MAC인지를 판단한다(S134). 여기서, 차단MAC 이란 통신제어장치 EQ-X가 신차단을 위해 의도적으로 조작한 MAC 어드레스이다. 차단 MAC이 아닌 경우라면, 단이 되어 있지 않은 상태이어서 해제의 필요성도 없으므로 그냥 무시하면 된다 136). 그러나 차단 MAC인 경우에는 현재 통신차단이 된 상태이므로, 통신제어장치 -X는 데이터링크 레이어 어드레스를 통신제어룰 DB에 조회하여 등록된 통신제어룰 비교한다(S138). 비교결과 여전히 통신차단의 대

으로 확인되면 그 상태를 그대로 유지하면 되며, 네트워크의 관리목적으로 검출시을 어드레스 DB에 업데이트 해둔다(S142). 하지만 위 비교결과, 설정된 통신제어물 통신차단의 해제 대상이면 통신제어장치는 해제를 위한 ARP 패킷을 망내 모든 장들에게 유니캐스트 방식으로 송신하여 통신차단상태가 해제되도록 한다(S140). 통차단을 해제하기 위해 송신되는 ARP 패킷에는 정상적인 MAC 어드레스가 포함되어으므로, 이를 수신한 망내 장비들은 이후 그 MAC 어드레스를 가진 장비에 대해서는신을 정상적으로 할 수 있게 된다. 이로써 통신차단상태는 해제된다.

도 8은 통신제어물 DB에 설정된 룰에 따라 망내 장비들 간의 통신제어가 처리되절차를 도시한다. 네트워크 내의 어떤 장비 EQ-i가 망내 다른 장비들과 통신을 하위해 네트워크 레이어 패킷을 브로드캐스팅 방식으로 송신하면(S150), 통신제어장는 그 네트워크 레이어 패킷을 검출하여(S152), 그 패킷에 내포된 데이터링크 레이어드레스가 차단 MAC인지를 판단한다(S154). 차단 MAC이 아니면 통신을 차단할 대이 아니므로 무시하면 된다(S156). 그러면 그 데이터링크 레이어 어드레스를 가진비와 통신을 요청한 장비 EQ-i 간에는 정상적인 통신이 이루어질 것이다. 하지만이터링크 레이어 어드레스가 차단 MAC인 경우에는 통신을 통제해야 할 대상이므로, 신제어장치는 데이터링크 통신제어물 DB에 등록된 통신제어물과 비교하여(S158, 60) 어떤 통제를 가할 지를 판별한다. 통신차단의 대상으로 설정된 경우에는 앞서명한 바 있는 조작된 ARP 패킷의 송신에 의해 통신이 차단될 수 있도록 처리한다162). 만약 통신이 허용되는 것으로 설정된 경우라면, 원래의 목적지로 네트워크이어 패킷을 포워딩한다(S164).

도 9는 패킷의 검출과 그에 따른 어드레스 수집 절차에 대해 보다 구체적으로 타내고 있다. 네트워크 레이어 어드레스와 데이터링크 레이어 어드레스 수집 루트 크게 두 가지가 있다. 도 19에 도시된 것처럼, 하나는 통신제어장치 EQ-X가 관리상 DB에 있는 어드레스를 참조하여 ARP 요청 패킷을 브로드캐스팅 방식으로 발송하(S170, S172). 발송된 ARP 요청패킷에 내포된 프로토콜 어드레스를 가진 망내 장비 ARP 응답패킷으로 응답하면 통신제어장치가 그 응답패킷으로부터 어드레스를 수집는 것이다(S174, S178). 다른 하나는, 이러한 요청절차 없이, 망내 장비들끼리 통을 하기 위해서는 ARP 패킷을 브로드캐스팅 방식으로 네트워크에 전송하는데, 그렇 발생된 ARP 패킷을 통신제어장치가 검출함으로써 그 검출된 ARP 패킷으로부터 어레스를 검출한다(S176, S178). 검출된 어드레스는 그대로 어드레스관련 DB에 저장리하며, 이때 관리목적상 검출시간도 함께 저장한다.

다음으로, 에이전트 프로그램의 차단/해제 관리모듈은 다음과 같은 처리를 한다 검출된 패킷에 따른 통신 제어 처리, ARP 요청(Request)패킷 검출에 따른 처리, P 응답(Reply)패킷 검출에 따른 처리, 프로토콜 레이어 검출에 따른 처리, 프로토 어드레스 및 데이터링크 레이어 어드레스에 의한 관리룰 검색, 프로토콜어드레스 의한 관리룰 검색 등이다. 이에 관해 보다 구체적으로 설명한다.

도 10은 검출된 패킷에 따른 통신제어처리 절차를 도시한다. 검출된 패킷이 IP 킷인지 아니면 ARP 패킷인지에 따라서 후속 처리 내용이 다르게 결정된다. 통신제 장치 EQ-X가 어떤 루트에 의해서건 네트워크로부터 패킷을 검출하게 되면(S180), 출된 패킷이 IP 패킷인지 혹은 ARP 패킷인지를 조사한다(S182). ARP 패킷이면 ARP 청패킷 검출에 따른 루틴과 ARP 응답패킷 검출에 따른 루틴을 실행한다(S184). IP

킷인 경우에는 다시, 그 패킷의 이더넷 목적지 어드레스가 차단어드레스인지를 체
한다(S186). 차단어드레스는 통신제어장치에 의해 조작된 어드레스이므로, 이에 해
되지 않는다면 정상적인 통신이 보장될 필요가 있으므로 통신제어장치는 아무런 액
을 취하지 않고 무시하기만 하면 된다(S188). 차단어드레스인 경우는 통신제어장치
통신차단을 위한 처리를 수행해야 한다. 이를 위해 프로토콜 레이어 패킷을 처리
는 루틴을 실행함으로써, 해제모듈과 패킷포워딩모듈 중 어느 하나가 실행되도록
다(S189).

도 11은 도 10의 S184 단계의 'ARP 요청패킷의 검출에 따른 처리 루틴'을 보다
체적으로 나타낸다. ARP 요청패킷은 일반적으로 브로드캐스팅 방식으로 전송된다.
내 특정 장비가 다른 장비와 통신을 하기 위해 ARP 요청패킷을 브로드캐스팅하면,
신제어장치 EQ-X가 그 ARP 요청패킷을 검출하게 된다(S190). 검출된 ARP 요청패킷
내포된 어드레스를 추출하여 프로토콜어드레스DB (DB-1), 데이터링크-MAC어드레스
B (DB-2), 프로토콜-데이터링크 레이어 어드레스 DB (DB-3)와 같은 어드레스 DB에
규로 생성하거나 수정 하는 등의 반영을 한다(S192). 그런 다음, 먼저 검출된 어드
스 중에서 수신측 어드레스를 가지고서 통신차단을 위한 처리를 한다(S194, S196,
98). 이를 위해 먼저 통신제어장치는 수신측 어드레스를 이용하여 그에 관한 관리
이 존재하는지를 검색하여(S194), 수신측 어드레스가 차단대상인 경우 즉, 차단을
존재하는 경우에는 프로토콜 데이터링크 레이어 어드레스

(DB-3)를 이용하여 수신 프로토콜 어드레스와 '같은 것들'에 대해서 차단패킷을 송
하는 처리를 수행한다(S198). 통신제어장치는 예컨대 수신 프로토콜 어드레스가
T-1과 NET-3이면, 같은 프로토콜 어드레스를 갖는 장비 EQ-1과 EQ-3에 대하여 차단
킷을 송신한다. 예컨대 NET-3이 차단대상인 경우를 가정하면, 장비 EQ-1이 장비
-3과 통신을 원할 때 장비 EQ-1이 브로드캐스팅 한 ARP 요청 패킷을 통신제어장치
수신하게 되는데, 이 경우 통신제어장치는 EQ-1과 EQ-3에게 ARP 패킷을 보낸다.
송하는 ARP 패킷에 의하면, EQ-1에 대해서는 EQ-3이 통신제어장치인 것처럼 거짓
드레스정보가 제공되고, EQ-3에 대해서는 EQ-1이 통신제어장치인 것처럼 거짓 어드
스정보가 제공된다. 이에 의해 장비 EQ-1과 EQ-3이 보낸 패킷은 통신제어장치 EQ-X
게 전달되어 무시되므로 양 장비 간의 통신은 차단된다. 수신측 어드레스를 이용한
리가 끝난 다음에는 송신측 어드레스에 대하여도 통신차단을 위한 처리를 한다
200, S202, S204). 수신측 어드레스를 이용한 차단패킷의 송신과 거의 유사하나,
가지 차이점은 차단패킷의 송신 대상이 송신측 프로토콜과 동일한 네트워크에 속
는 '모든' 프로토콜-데이터링크 레이어 어드레스 DB(DB-3)라는 점이다. 왜냐하면
신측이 브로드캐스팅 한 ARP 요청패킷은 망내 모든 장비에 대하여 영향을 주기 때
이다.

도 12는 도 10의 S184 단계의 'ARP 응답패킷의 검출에 따른 처리 루틴'을 보다
체적으로 나타낸다. 통신제어장치가 보낸 ARP 요청패킷에 응하여 망내 장비가 ARP
답패킷을 보내오면 통신제어장치는 이를 검출하여(S210), 그 속에 내포된 어드레스
추출하여 프로토콜어드레스DB (DB-1), 데이터링크-MAC어드레스 DB (DB-

. 프로토콜-데이터링크 레이어 어드레스 DB (DB-3)와 같은 어드레스 DB에
영한다(S212). ARP 응답패킷은 일반적으로 유니캐스트 방식으로 전송된다. 따라서 출된 응답패킷이 유니캐스트 방식으로 전송된 패킷인 경우는 정상적인 것이므로 그 답패킷에 대하여 통신제어장치가 예정한 후속 처리를 적절히 수행하면 된다(S214. 16). 하지만 그 응답패킷이 브로드캐스트 방식의 패킷인 경우는 망내 다른 장비들게 전달되지 않아야 될 것이 비정상적으로 전달된 경우에 해당된다. 그러므로 적절 후속절차가 필요하다. 즉. 검출된 응답패킷에 포함되어 있는 송신측 어드레스를 용하여 관리툴을 검색하고(S218). 검색결과 그 송신측 어드레스에 대하여 차단툴이 재하면 송신측 프로토콜과 동일한 네트워크에 속하는 모든 프로토콜-데이터링크 레어 어드레스DB(DB-3)에 대하여 차단패킷을 송신하는 처리를 수행한다(S220. S222). 답패킷이 브로드캐스트 되었기 때문에 망내 모든 장비가 그 패킷의 영향을 받게 되 . 그로 인한 통신이 일어날 수 있는데. 그 경우 통신차단의 대상들끼리는 통신이 루어지지 않도록 하는 조치가 개입되어야 하기 때문이다.

도 13은 프로토콜 레이어 패킷의 검출에 따른 처리 절차를 도시한다. 이는 도의 S189단계에 대응된다. 통신제어장치가 프로토콜 레이어 패킷을 검출하게 되면 230). 그 패킷에 포함된 이더넷 목적지 어드레스가 차단어드레스인지를 체크한다 232). 이러한 체크 결과에 따라 통신제어장치가 후속적으로 수행하여야 할 처리 내은 통신차단의 해제. 패킷포워딩. 그리고 그 패킷을 무시하는 것이다. 이더넷 목적가 차단어드레스가 아닌 경우에는 정상적인 통신이 보장되어야 하므로.

냥 무시하면 된다(S234). 이더넷 목적지 어드레스가 차단어드레스인 경우는 통신제
장치가 조작된 MAC 어드레스 즉, 송신측 MAC 어드레스를 통신제어장치로 설정해둔
킷을 해당 장비에게 미리 제공하여 그 장비에 대해 통신을 차단해둔 경우이다. 이
우에는 송신측 어드레스(프로토콜 및 데이터링크 레이어 어드레스)와 수신측 어드
스(프로토콜 및 데이터링크 레이어 어드레스)를 검출하고(S236), 송신측 어드레스
수신측 어드레스에 따라 통신의 허용, 차단 또는 패킷포워딩과 같은 처리를 한다.
저 통신제어장치는 송신측어드레스에 의한 관리룰을 검색하여(S238), 모두 차단으
설정되어 있는 경우에 통신제어장치는 해당 패킷을 무시 해버리면 된다(S240). 그
면 그 패킷은 통신제어장치를 벗어나지 못하여 통신이 근원적으로 차단된다. 송신
어드레스에 의한 관리룰이 일부 차단인 경우에는 수신측 어드레스와 통신이 가능
지 여부를 체크하고(S242), 차단으로 설정되어 있으면 무시 해버리고(S240), 통신
허용되면 수신측 어드레스에 의한 관리룰을 검색한다(S244). 마찬가지로 검색결과
2두 차단이면 그 패킷을 무시해버리면 되고(S246), 검색결과 일부차단인 경우에는
신측 어드레스와의 통신허용 여부를 체크한다(S248). 통신이 차단된 경우에는 당해
킷을 무시해버리면 된다. 통신이 허용되는 경우에는 프로토콜 레이어 패킷의 포워
루틴을 실행한다(S250). 그런 다음 통신차단이 잘못된 경우 통신차단상태를 해제
기 위한 패킷을 송신함으로써, 그러한 잘못된 상태를 바로잡는 절차를 수행한다
253). 이러한 해제처리에 의해 프로토콜 레이어 패킷은 더 이상 통신제어장치로 전
되지 않고 정상적인 목적지로 송신된다.

도 14는 도 13의 패킷포워딩 단계(S250)를 보다 구체적으로 나타낸 흐름도이다.
킷포워딩 절차에 있어서, 통신제어장치가 수신측 데이터링크 레이어 어드레스가 차

어드레스인 프로토콜 레이어 패킷을 검출하면(S254). 송신측 어드레스와 수신측 드레스에 의한 차단 여부를 검색한다(S255). 검색결과 통신차단을 해야 할 어드레로 설정되어 있지 않는 경우에는 현재 통신이 차단된 상태는 잘못된 것이므로 그 신차단을 해제하기 위한 처리를 수행한다(S256). 반면에 통신차단으로 설정된 경우 그 패킷을 차단해야 할 것인지 아니면 포워딩 해야 할 것인지를 더 체크한다 257). 검색된 어드레스에 대하여 패킷포워딩 룰이 존재하는 경우에는 그 패킷의 목지 어드레스를 정상적인 데이터링크 레이어 어드레스로 하여 그 패킷을 포워딩 한(S259). 포워딩 룰이 존재하지 않는다면, 그 패킷은 정상적으로 차단시켜야 할 것므로 그 패킷을 다른 어떤 장비에도 전달하지 않고 무시해버린다(S258).

다음으로 도 15를 참조하여 ARP 응답패킷과 ARP 요청패킷의 검출에 따른 어드레 DB의 관리단계(예컨대 도 11의 S192 단계와 도 12의 S212 단계)의 절차를 도시한 . 어드레스 DB를 관리하는 이유는 망내 장비들에 대한 관리, 특히 통신제어를 하기 해서는 관리 및 제어의 대상인 망내 장비들에 대한 리스트 확보가 필요하며, 특히 재 전원이 켜져 정상적으로 작동하고 있는 장비들의 리스트를 알 필요가 있기 때문다. 통신제어장치가 망내 어떤 장비가 보낸 ARP 요청패킷이나 응답패킷을 검출하게 면(S260), 검출된 패킷 내의 자료 중에 내포된 송신자 프로토콜 어드레스가 프로콜어드레스 DB (DB-1) 내에 존재하는지 여부를 검사한다(S262). 존재하지 않는다면 l 어드레스는 새로운 것이므로 그 송신자 프로토콜 어드레스를 생성하고(S264), 존한다면 다음 단계로서 패킷 내의 자료 중의 송신자 데이터링크 레이어 어드레스가 이터링크 레이어 어드레스 DB (DB-2) 내에 존재하는지를 검사한다(S266). 존재하지 는다면 마찬가지로 송신자 데이터링크 레이어 어드레스를 생성하고(S268), 존재한

면 한 쌍의 송신자 프로토콜 어드레스-송신자 데이터링크 레이어 어드레스 조합이 로토콜-데이터링크 레이어 어드레스 DB(DB-3)에 존재하는지를 검사한다. 존재하지 는다면 그 프로토콜-데이터링크 레이어 어드레스 조합을 생성하고(S272), 존재한다 어드레스를 새로 생성시킬 필요는 없다. 다만 네트워크 상의 장비를 원활히 관리 목적으로, 통신제어장치는 그 장비로부터 패킷을 수신한 시간을 어드레스관리 DB 기록하여 그 장비의 최근의 활동시간을 알 수 있도록 한다.

다음으로, 네트워크 관리자는 프로토콜 어드레스 또는 데이터링크 레이어 어드스에 대하여 개별적으로 통신제어룰을 설정할 수 있지만 이들 두 어드레스의 조합 대하여도 통신제어룰을 설정할 수가 있다. 도 16은 프로토콜 어드레스와 데이터링 레이어 어드레스의 조합에 대해 설정된 통신제어룰을 검색하여 처리하는 것을 도 하며, 도 17과 18은 프로토콜 어드레스와 데이터링크 레이어 어드레스에 의한 통신 어룰을 검색하여 처리하는 것을 도시한다.

도 16의 흐름도에 있어서, 먼저 통신제어장치가 패킷 내의 송신측 자료 또는 관자자 수동으로 입력한 자료로부터 프로토콜 어드레스와 데이터링크 레이어 어드레 를 검출한다(S280). 이렇게 어드레스 검출이 이루어진 다음, 프로토콜어드레

DB(DB-1)와 데이터링크-MAC 어드레스 DB(DB-2)에 조회하여 검출된 프로토콜 어드
스와 데이터링크 레이어 어드레스 그 자체가 차단대상인지 여부의 조회(S282). 데
터링크-MAC 어드레스 DB(DB-2)와 프로토콜-데이터링크 레이어 어드레스 DB (DB-3)
조회하여 검출된 프로토콜 어드레스와 다른 어드레스의 세트 그리고 검출된 데이
링크 레이어 어드레스와 다른 어드레스의 세트가 통신차단인지 여부의 조회(S286).
로토콜어드레스그룹 DB (DB-4). 데이터링크 레이어 어드레스그룹 DB (DB-5). ITEM
위 룰DB (DB-6)에 조회하여 검출된 프로토콜 어드레스와 데이터링크 레이어 어드레
각각에 대하여 관계룰에 의한 통신차단 대상에 해당하는지 여부의 조회(S290). 프
토콜어드레스그룹 DB (DB-4). 데이터링크 레이어 어드레스그룹 DB (DB-5). 그룹 간
룰DB (DB-7)에 조회하여 검출된 프로토콜 어드레스를 포함한 그룹과 검출된 데이
링크 레이어 어드레스를 포함한 그룹에 대하여 그룹룰에 의한 통신차단 대상에 해
하는지 여부의 조회(S294). 그리고 검출된 패킷에 대하여 패킷 포워딩 룰이 존재하
지 여부의 조회(S298). 등을 수행한다. 이러한 조회 결과, 차단대상으로 확인되면
신차단을 위한 처리를 한다. 이때, S282 단계와 S286 단계의 경우는 해당 어드레스
대한 전면적인 통신차단 조치를 취하면 되고(S284, S288). 단계 S290과 단계 S294
경우에는 관계 전체 또는 그룹 전체에 대한 통신차단을 하는 것이 아니라 그 관계
는 그룹 중 해당되는 어드레스에 대해서만 통신차단을 한다(S292, S296). 검출된
킷에 대하여 포워딩 룰이 존재하는 경우 그 패킷을 포워딩 처리를 하고(S300). 그
지 않는 경우에는 무시한다(S302).

도 17에 도시된 프로토콜 어드레스에 의한 통신제어룰의 처리를 설명하면,

신제어장치가 수신한 패킷 내의 수신측 프로토콜 어드레스 또는 관리자자 수동으로 입력한 자료로부터 프로토콜 어드레스를 검출하여(S310) 프로토콜어드레스 DB(DB-1) 그 검출된 프로토콜 어드레스가 차단대상인지 여부를 조회한다(S312). 차단대상이 그 프로토콜 어드레스에 대한 통신을 완전히 차단하고(S314). 그렇지 않은 경우에 검출된 프로토콜 어드레스에 관련된 관계물에 의한 차단여부를 프로토콜어드레스 DB (DB-4). 데이터링크 레이어 어드레스그룹 DB (DB-5). ITEM단위 룰DB (DB-6) 조회한다(S316). 조회결과 관계물이 차단대상이면 검출된 프로토콜 어드레스에 관 된 것에 대해서만 한정적으로 통신을 차단한다(S318). 나아가 검출된 프로토콜 어 레스가 포함된 그룹에 대해서 그룹에 의한 차단여부를 프로토콜어드레스그룹 DB B-4). 데이터링크 레이어 어드레스그룹 DB (DB-5). 그룹 간의 룰DB (DB-7)에 조회 다(S320). 조회결과 그룹룰이 차단대상이면 검출된 프로토콜 어드레스에 관련된 것 대해서만 한정적으로 통신을 차단한다(S322). 또한 검출된 패킷에 대하여 포워딩 이 존재하는 경우 그 패킷을 포워딩 처리를 하고(S326). 그렇지 않는 경우에는 무 한다(S328).

데이터링크 레이어 어드레스에 의한 통신제어룰의 처리에 관해서는 비슷하게 수 되는데, 도 18에 도시된 흐름도를 참조하면 쉽게 이해가 될 수 있으므로 여기서는 에 관한 설명을 생략한다.

이상에서 설명한 바와 같이, 본 발명은 네트워크의 자원관리 소프트웨어로 구현 수 있으며, 이를 설치한 컴퓨터 시스템을 네트워크 통신제어장치로 이용할 수 있

발명의 효과】

본 발명은 복잡 다양화되어 가는 네트워크 환경하에서 제한된 인적자원을 통해 대한 네트워크 자원을 효율적이고 통합적인 관리와 제어가 가능하며, 인트라넷 ntranet) 상의 모든 사용자에 대한 보안 통제기능을 확보할 수 있다. 구체적으로, 발명을 이용하면 다음과 같은 효과를 얻을 수 있다.

첫째, 네트워크 운용의 효율화를 도모할 수 있다. 즉, 네트워크 리소스에 대한 보를 자동으로 수집할 수 있고, 장애 발생에 관한 정보를 실시간으로 모니터링할 있으므로 장애에 대한 신속한 조치가 가능하다. 또한 네트워크상에서 내부/외부 신 데이터 패킷을 선별적으로 제어 통제함으로써 외부 네트워크를 담당하는 네트워 장비의 리소스를 절약할 수 있으며, 방화벽 서버의 리소스의 경감으로 외부 통신 도 증가를 가져올 수 있다. 나아가, 각 네트워크 별로 사용제한을 할 수 있는 등, 트워크를 효율적으로 운용할 수 있는 수단을 확보할 수 있게 된다.

둘째, 네트워크 내부의 보안을 강화할 수 있다. 즉, 외부 네트워크의 접근을 제 할 수 있을 뿐만 아니라 내부 네트워크 간의 접근을 제한 할 수 있고, 특정 서버 접근도 제한 할 수 있다. 그러므로 일반적인 방화벽 서버에서는 처리할 수 없는 트워크 내부 장비들 간의 통신제어를 할 수 있을 뿐만 아니라, 특정 서버의 IP보호 부정 내부 이용자끼리 정보의 유출이나, 해킹, 크래킹을 방지할 수 있으며, 이로 한 데이터 패킷의 감소를 유도할 수 있다.

세째로 네트워크의 안정적인 운영을 도모할 수 있다. 네트워크 내의 장비나 리 스에 대한 정보수집과 네트워크 상황에 대한 정보를 모니터링 하고, 수집 분석함으

써 장애 발생 전에 경고하거나 장애 발생요소를 사전에 제거할 수 있고, 나아가 장애 발생 시 원인파악과 조치가 신속히 이루어질 수 있다.

네째, IP 충돌을 효과적으로 해결할 수 있다. MAC 어드레스뿐만 아니라 IP 어드레스도 조작이 가능하므로, 네트워크 내 장비들 간의 IP 어드레스의 충돌이 발생하는 경우 올바른 IP어드레스를 해당 장비에게 제공하여 IP어드레스의 충돌도 자동으로 해결할 수 있다.

이상에서는 본 발명의 바람직한 실시예를 참조하여 설명하였지만, 해당 기술분야의 숙련된 당업자는 하기의 특허청구의 범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있다. 따라서 특허청구범위의 등가적인 의미나 범위에 속하는 모든 변화들은 전부 본 발명의 특허범위안에 속함을 밝혀둔다.

【특허청구범위】

【청구항 1】

특정 네트워크 상의 장비들 간의 통신을 제어하는 방법에 있어서,

상기 네트워크 상의 장비들과 동일 레벨에 위치한 통신제어장비를 이용하여, 통신차단 대상인 장비들에 대하여 데이터링크 레이어 어드레스가 조작된 ARP 패킷을 제공하여 상기 차단대상 장비가 송신한 데이터 패킷이 비정상적인 어드레스로 전송되도록 함으로써 상기 차단대상 장비들 간의 통신을 차단하는 것을 특징으로 하는 통신제어방법.

【청구항 2】

제 1항에 있어서, 통신차단의 대상이 아님에도 불구하고 통신차단상태에 있는 장비에 대해서는 상기 통신제어장치가 정상적인 어드레스 정보를 내포하는 ARP패킷을 당 장비에게 송신함으로써 그러한 통신차단상태를 해제 단계를 더 구비하는 것을 특징으로 하는 통신제어방법.

【청구항 3】

제 1항에 있어서, 상기 차단대상 장비들 간의 통신을 차단하기 위해 상기 차단대상 장비의 일부 또는 전부의 데이터링크 레이어 어드레스를 상기 통신제어장비 데이터링크 레이어 어드레스 또는 상기 차단대상 장비의 것이 아닌 제3의 데이터링크 레이어 어드레스로 설정하는 것을 특징으로 하는 통신제어방법.

청구항 4】

제 1항에 있어서, 네트워크에 신규로 연결된 장비의 IP 어드레스를 기존 장비들 IP 어드레스와 비교하여 충돌이 있는 경우, 올바른 IP 어드레스를 유니캐스트로 존 장비에 전달하여 IP어드레스의 충돌을 해결하는 단계를 더 구비하는 것을 특징로 하는 통신제어방법.

청구항 5】

특정 네트워크 상의 장비들 간의 통신을 제어하는 방법에 있어서,

통신제어장치가 네트워크 내에 존재하는 네트워크 레이어 어드레스(이더넷 아피 어드레스)와 데이터링크 레이어 어드레스(MAC:media access control)를 수집하 단계;

네트워크 관리자가 수집된 어드레스에 대하여 원하는 통신제어를 하기 위해 설한 통신제어룰을 DB에 저장하는 단계;

네트워크 내의 어떤 장비가 망내 다른 장비와 통신을 하기 위해 송신한 어드레결정프로토콜(ARP) 패킷을 검출하는 단계;

통신제어룰 데이터베이스에 조회하여 검출된 ARP 패킷이 통신차단대상에 해당하지를 판별하는 단계; 및

통신차단대상에 해당하는 경우 통신차단을 위한 ARP패킷을 만들어 송신하는 단를 구비하여 망내 장비들 간의 통신을 필요에 따라 선택적으로 제어할 수 있는 것 특징으로 하는 통신제어방법.

구항 6】

제 5항에 있어서, 상기 어드레스 수집단계는 상기 네트워크의 어떤 장비가 망내 른 장비와 통신하기 위해 브로드캐스팅 한 ARP 패킷을 상기 통신제어장치가 수신 여 그 ARP 패킷에 내포된 네트워크 레이어 어드레스와 데이터링크 레이어 어드레스 검출하는 방법 및/또는 네트워크 관리자가 직접 입력한 관리대상 장비의 어드레스 의거하여 상기 통신제어장치가 ARP 요청패킷을 송신하고 이에 응하여 관리대상 장 가 보내온 ARP 응답패킷으로부터 네트워크 레이어 어드레스와 데이터링크 레이어 드레스를 검출하는 방법에 따르는 것을 특징으로 하는 통신제어방법.

구항 7】

제 5항에 있어서, 상기 통신제어툴의 설정 대상은 네트워크 레이어 어드레스 상 간, 데이터링크 레이어 어드레스 상호간, 네트워크 레이어 어드레스와 데이터링크 이어 어드레스 상호간의 통신인 것을 특징으로 하는 통신제어방법.

구항 8】

제 7항에 있어서, 상기 통신제어툴의 설정 대상은 네트워크 레이어 어드레스와 트워크 레이어 어드레스 그룹 상호간, 데이터링크 레이어 어드레스와 데이터 링크 이어 어드레스 그룹 상호간, 네트워크 레이어 어드레스와 데이터 링크 레이어 어드 스 그룹 상호간, 데이터링크 레이어 어드레스와 네트워크 레이어 어드레스 그룹 상 간, 네트워크 레이어 어드레스 그룹과 데이터 링크 레이어 어드레스 그룹 상호간의 통신을 더 포함하는 것을 특징으로 하는 통신제어방법.

【구항 9】

제 5항에 있어서, 수신측 어드레스가 차단대상인 경우에는 수신 프로토콜 어드스와 '같은 것들'에 대해서 차단패킷을 송신하는 것을 특징으로 하는 통신제어방

【구항 10】

제 5항에 있어서, 송신측 어드레스가 차단대상인 경우에는 송신측 프로토콜과 일한 네트워크에 속하는 '모든' 프로토콜-데이터링크 레이어 어드레스에 대하여 차패킷을 송신하는 것을 특징으로 하는 통신제어방법.

【구항 11】

제 5항에 있어서, 통신제어장비가 보낸 ARP 요청패킷에 응하여 망내 장비가 ARP 답패킷을 보내오면 검출된 응답패킷에 포함되어 있는 송신측 어드레스를 이용하여 리를을 검색하고, 검색결과 그 송신측 어드레스에 대하여 차단룰이 존재하면 송신 프로토콜과 동일한 네트워크에 속하는 모든 프로토콜-데이터링크 레이어 드레스DB(DB-3)에 대하여 차단패킷을 송신하는 단계를 더 구비하는 것을 특징으로는 통신제어방법.

【구항 12】

제 5항에 있어서, 네트워크 레이어 패킷의 검출에 따라 더 이상 통신차단의 대이 아님에도 불구하고 여전히 통신차단상태로 되어 있는 장비에 대해 그러한 통신단상태의 해제를 위한 ARP패킷을 만들어 송신하는 단계를 더 구비하는 것을 특징으하는 통신제어방법.

청구항 13】

제 5 또는 제 12항에 있어서, 일정한 시간 마다 통신제어룰 데이터베이스에 따 통신차단/통신차단해제를 위한 ARP요청 패킷을 송신하는 단계를 더 구비하는 것을 특징으로 하는 통신제어방법.

청구항 14】

제 5항에 있어서, 수신측 데이터링크 레이어 어드레스가 차단 어드레스로서 패 포워딩 룰이 존재하는 경우 수신된 프로토콜 레이어 패킷을 그 패킷의 목적지 어드스를 정상적인 데이터링크 레이어 어드레스로 하여 포워딩 하는 단계를 더 구비하 것을 특징으로 하는 통신제어방법.

청구항 15】

제 5항에 있어서, 네트워크에 신규로 연결된 장비의 IP 어드레스를 기존 장비들 IP 어드레스와 비교하여 충돌이 있는 경우, 올바른 IP 어드레스를 유니캐스트로 존 장비에 전달하여 IP어드레스의 충돌을 해결하는 단계를 더 구비하는 것을 특징로 하는 통신제어방법.

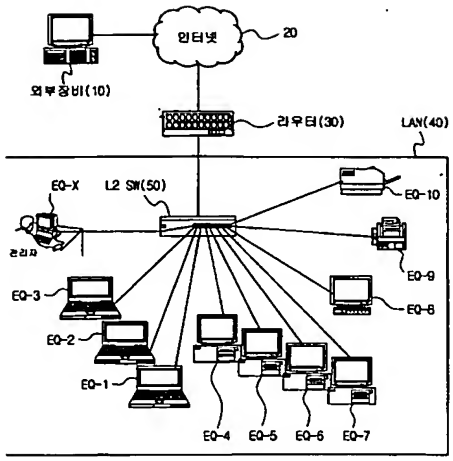
청구항 16】

어떤 네트워크 상의 다른 장비들과 동일레벨에 위치하면서, 네트워크 관리자가 요에 따라 상기 다른 장비들 상호간의 통신을 차단할 수 있는 통신제어룰을 설정할 있는 환경을 제공하고, 설정된 상기 통신제어룰을 데이터베이스에 저장 관리하면 , 통신차단 대상으로 설정된 장비들에 대하여 데이터링크 레이어 어드레스가 조작 ARP 패킷을 제공하여 상기 차단대상 장비가 송신한 데이터 패킷이 비정상적인 어

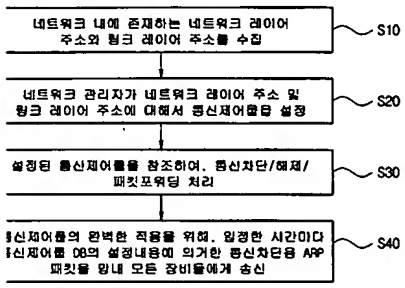
레스로 전송되도록 함으로써 상기 차단대상 장비들 간의 통신을 차단하는 것을 특
으로 하는 통신제어장치.

【도면】

【도 1】

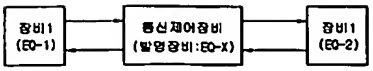

인터넷
20
외부장비(10)
라우터(30)
LAN(40)
EQ-X
L2 SW(50)
EQ-10
관리자
EQ-9
EQ-3
EQ-8
EQ-2
EQ-1
EQ-4
EQ-5
EQ-6
EQ-7

【도 2】

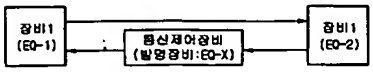

네트워크 내에 존재하는 네트워크 레이어 주소와 링크 레이어 주소를 수집
S10
네트워크 관리자가 네트워크 레이어 주소 및 링크 레이어 주소에 대해서 통신제어룰을 설정
S20
설정된 통신제어룰을 참조하여, 통신차단/해제/패킷포워딩 처리
S30
통신제어룰의 완벽한 적용을 위해, 일정한 시간이다 통신제어룰 DB의 설정내용에 의거한 통신차단용 APP 패킷을 망내 모든 장비들에게 송신
S40

도 3]

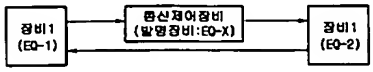
a)


장비1
(EQ-1)
통신제어장비
(발명장비:EQ-X)
장비1
(EQ-2)

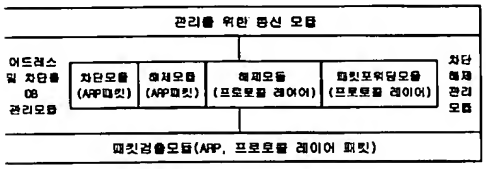
b)


장비1
(EQ-1)
통신제어장비
(발명장비:EQ-X)
장비1
(EQ-2)

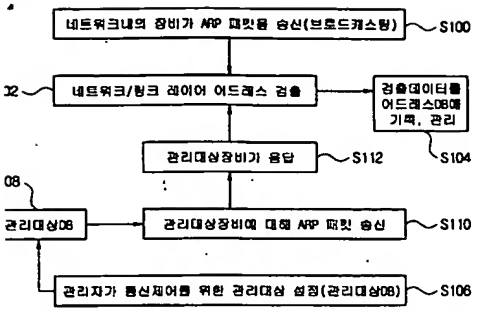
c)


장비1
(EQ-1)
통신제어장비
(발명장비:EQ-X)
장비1
(EQ-2)

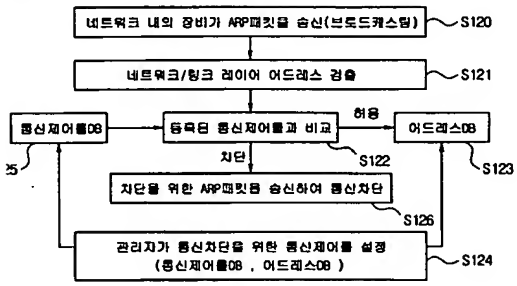
도 4]


관리를 위한 통신 모듈
어드레스 및 차단을 DB 관리모듈
차단모듈 (APP패킷)
해제모듈 (APP패킷)
해제모듈 (프로토콜 레이어)
패킷포워딩모듈 (프로토콜 레이어)
차단 해제 관리 모듈
패킷검출모듈(APP, 프로토콜 레이어 패킷)

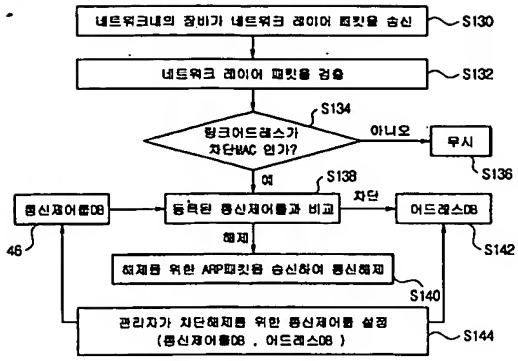
[도 5]


네트워크내의 장비가 ARP 패킷을 송신(브로드캐스팅)
S100
네트워크/링크 레이어 어드레스 검출
검출데이터를 어드레스DB에 기록, 관리
S104
관리대상장비가 응답
S112
관리대상장비에 대해 ARP 패킷 송신
S110
관리자가 통신제어를 위한 관리대상 설정(관리대상DB)
S106

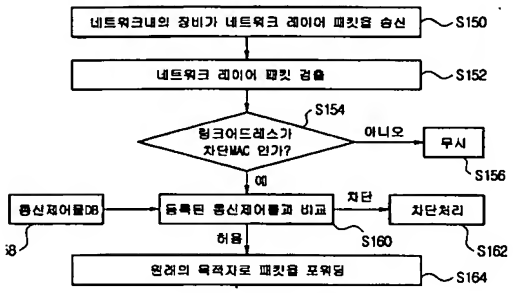
[도 6]


네트워크 내의 장비가 ARP패킷을 송신(브로드캐스팅)
S120
네트워크/링크 레이어 어드레스 검출
S121
통신제어를DB
등록된 통신제어룰과 비교
허용
어드레스DB
S122
S123
차단
차단을 위한 ARP패킷을 송신하여 통신차단
S126
관리자가 통신차단을 위한 통신제어룰 설정
(통신제어룰DB , 어드레스DB)
S124

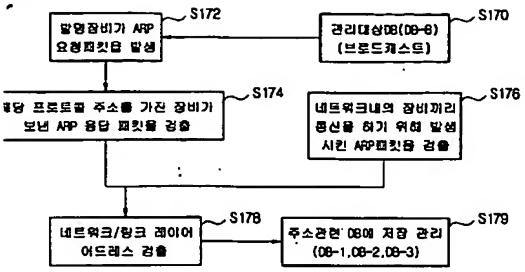
도 7]


네트워크내의 장비가 네트워크 레이어 패킷을 송신
S130
네트워크 레이어 패킷을 검출
S132
S134
링크어드레스가 차단MAC 인가?
아니오
무시
S136
예
S138
통신제어물DB
등록된 통신제어물과 비교
차단
어드레스DB
해제
S142
46
해제를 위한 ARP패킷을 송신하여 통신해제
S140
관리자가 차단해제를 위한 통신제어물 설정 (통신제어물DB , 어드레스DB)
S144

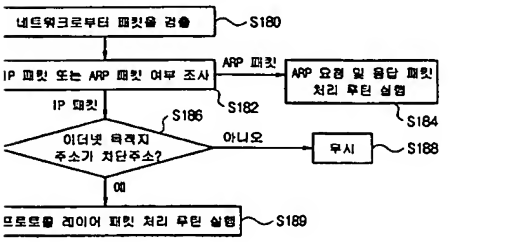
도 8]


네트워크내의 장비가 네트워크 레이어 패킷을 송신
S150
네트워크 레이어 패킷 검출
S152
S154
링크어드레스가 차단MAC 인가?
아니오
무시
S156
예
통신제어물DB
등록된 통신제어물과 비교
차단
차단처리
S162
허용
S160
원래의 목적지로 패킷을 포워딩
S164

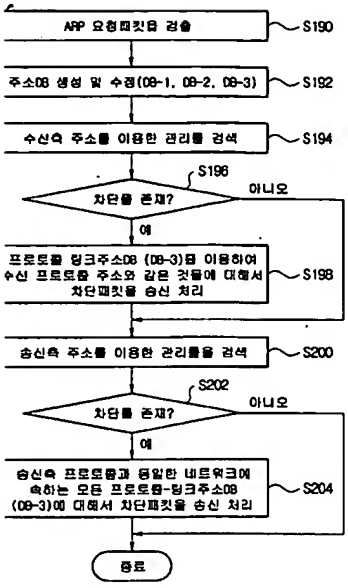
도 9]


발명장비가 ARP 요청패킷을 발생
S172
관리대상DB(DB-B) (브로드캐스트)
S170
해당 프로토콜 주소를 가진 장비가 보낸 ARP 응답 패킷을 검출
S174
네트워크내의 장비끼리 통신을 하기 위해 발생시킨 ARP패킷을 검출
S176
네트워크/링크 레이어 어드레스 검출
S178
주소관련 DB에 저장 관리 (DB-1,DB-2,DB-3)
S179

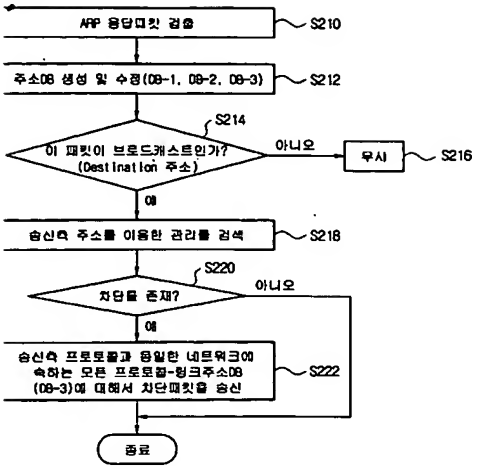
도 10]


네트워크로부터 패킷을 검출
S180
IP 패킷 또는 ARP 패킷 여부 조사
ARP 패킷
ARP 요청 및 응답 패킷 처리 루틴 실행
S184
S182
IP 패킷
S186
이더넷 목적지 주소가 차단주소?
아니오
무시
S188
예
프로토콜 레이어 패킷 처리 루틴 실행
S189

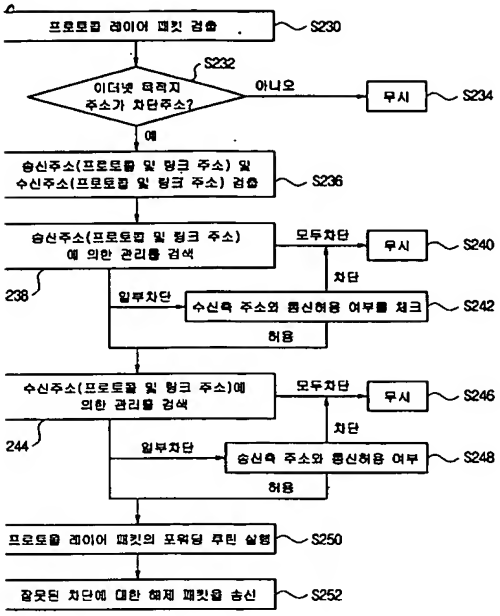
[도 11]


ARP 요청패킷을 검출
S190
주소DB 생성 및 수정(DB-1, DB-2, DB-3)
S192
수신측 주소를 이용한 관리를 검색
S194
S196
차단을 존재?
아니오
예
프로토콜 링크주소DB (DB-3)를 이용하여 수신 프로토콜 주소와 같은 것들에 대해서 차단패킷을 송신 처리
S198
송신측 주소를 이용한 관리를을 검색
S200
S202
차단을 존재?
아니오
예
송신측 프로토콜과 동일한 네트워크에 속하는 모든 프로토콜-링크주소DB (DB-3)에 대해서 차단패킷을 송신 처리
S204
종료

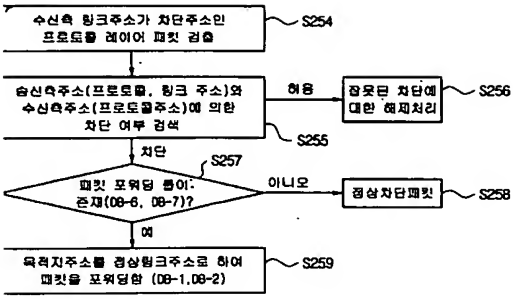
도 12]


ARP 응답패킷 검출
S210
주소DB 생성 및 수정(DB-1, DB-2, DB-3)
S212
S214
이 패킷이 브로드캐스트인가?
(Destination 주소)
아니오
무시
S216
예
송신측 주소를 이용한 관리를 검색
S218
S220
차단을 존재?
아니오
예
송신측 프로토콜과 동일한 네트워크에
속하는 모든 프로토콜-링크주소DB
(DB-3)에 대해서 차단패킷을 송신
S222
종료

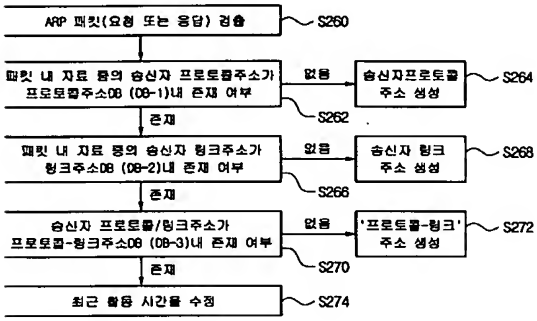
[도 13]


프로토콜 레이어 패킷 검출
S230
이더넷 목적지 주소가 차단주소?
S232
아니오
무시
S234
예
송신주소(프로토콜 및 링크 주소) 및 수신주소(프로토콜 및 링크 주소) 검출
S236
송신주소(프로토콜 및 링크 주소)에 의한 관리를 검색
모두차단
무시
S240
차단
238
일부차단
수신측 주소와 통신허용 여부를 체크
S242
허용
수신주소(프로토콜 및 링크 주소)에 의한 관리를 검색
모두차단
무시
S246
차단
244
일부차단
송신측 주소와 통신허용 여부
S248
허용
프로토콜 레이어 패킷의 포워딩 루틴 실행
S250
잘못된 차단에 대한 해제 패킷을 송신
S252

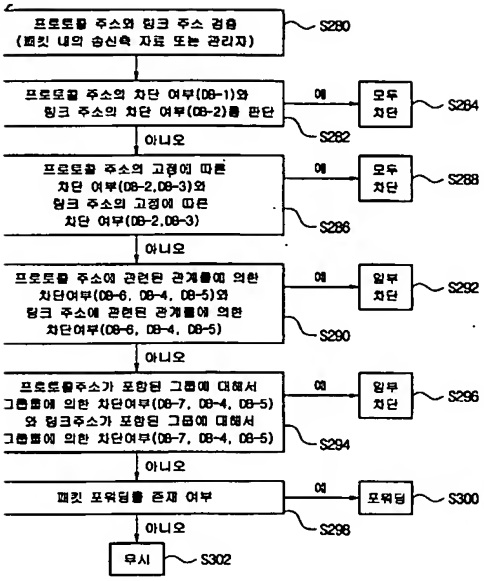
도 14]


수신측 링크주소가 차단주소인 프로토콜 레이어 패킷 검출
S254
송신측주소(프로토콜, 링크 주소)와 수신측주소(프로토콜주소)에 의한 차단 여부 검색
허용
잘못된 차단에 대한 해제처리
S256
S255
차단
S257
패킷 포워딩 룰이 존재(DB-6, DB-7)?
아니오
정상차단패킷
S258
예
목적지주소를 정상링크주소로 하여 패킷을 포워딩함 (DB-1,DB-2)
S259

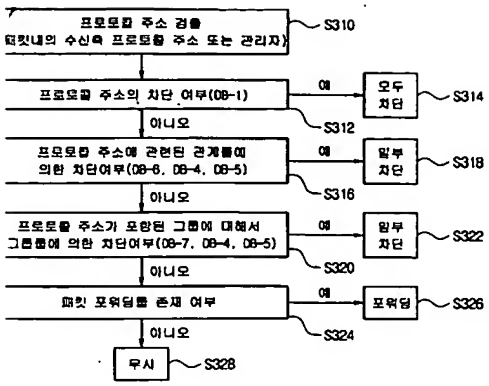
도 15]


ARP 패킷(요청 또는 응답) 검출
S260
패킷 내 자료 등의 송신자 프로토콜주소가 프로토콜주소DB (DB-1)내 존재 여부
없음
송신자프로토콜 주소 생성
S264
S262
존재
패킷 내 자료 등의 송신자 링크주소가 링크주소DB (DB-2)내 존재 여부
없음
송신자 링크 주소 생성
S268
S266
존재
송신자 프로토콜/링크주소가 프로토콜-링크주소DB (DB-3)내 존재 여부
없음
'프로토콜-링크' 주소 생성
S272
S270
존재
최근 활용 시간을 수정
S274

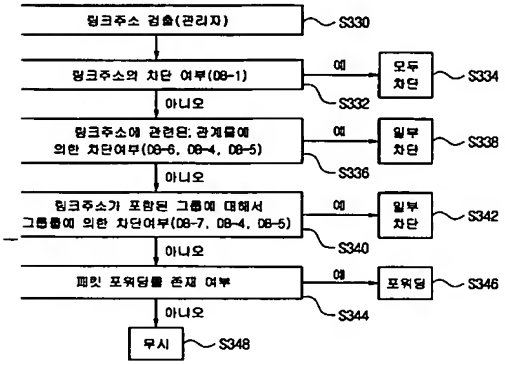
도 16)


프로토콜 주소와 링크 주소 검출
(패킷 내의 송신측 자료 또는 관리자)
S280
프로토콜 주소의 차단 여부(DB-1)와
링크 주소의 차단 여부(DB-2)를 판단
예
모두 차단
S284
S282
아니오
프로토콜 주소의 고정에 따른
차단 여부(DB-2,DB-3)와
링크 주소의 고정에 따른
차단 여부(DB-2,DB-3)
예
모두 차단
S288
S286
아니오
프로토콜 주소에 관련된 관계룰에 의한
차단여부(DB-6, DB-4, DB-5)와
링크 주소에 관련된 관계룰에 의한
차단여부(DB-6, DB-4, DB-5)
예
일부 차단
S292
S290
아니오
프로토콜주소가 포함된 그룹에 대해서
그룹룰에 의한 차단여부(DB-7, DB-4, DB-5)
와 링크주소가 포함된 그룹에 대해서
그룹룰에 의한 차단여부(DB-7, DB-4, DB-5)
예
일부 차단
S296
S294
아니오
패킷 포워딩룰 존재 여부
예
포워딩
S300
S298
아니오
무시
S302

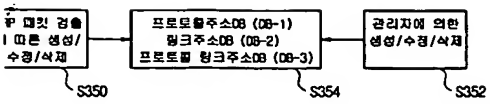
[도 17]


프로모컵 주소 검출
(패킷내의 수신측 프로모컵 주소 또는 관리자)
S310
프로모컵 주소의 차단 여부(DB-1)
예
오두 차단
S314
아니오
S312
프로모컵 주소에 관련된 관계들에 의한 차단여부(DB-6, DB-4, DB-5)
예
일부 차단
S318
아니오
S316
프로모컵 주소가 포함된 그룹에 대해서 그룹에 의한 차단여부(DB-7, DB-4, DB-5)
예
일부 차단
S322
아니오
S320
패킷 포워딩를 존재 여부
예
포워딩
S326
아니오
S324
무시
S328

[도 18]


링크주소 검출(관리자)
S330
링크주소의 차단 여부(DB-1)
예
오두 차단
S334
아니오
S332
링크주소에 관련된 관계들에 의한 차단여부(DB-6, DB-4, DB-5)
예
일부 차단
S338
아니오
S336
링크주소가 포함된 그룹에 대해서 그룹에 의한 차단여부(DB-7, DB-4, DB-5)
예
일부 차단
S342
아니오
S340
패킷 포워딩를 존재 여부
예
포워딩
S346
아니오
S344
무시
S348

도 19]


IP 매칭 검출
에 따른 생성/
수정/삭제
S350
프로모션주소DB (DB-1)
링크주소DB (DB-2)
프로모션 링크주소DB (DB-3)
S354
관리자에 의한
생성/수정/삭제
S352

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/KR04/002367

International filing date: 16 September 2004 (16.09.2004)

Document type: Certified copy of priority document

Document details: Country/Office: KR
Number: 10-2003-0065249
Filing date: 19 September 2003 (19.09.2003)

Date of receipt at the International Bureau: 04 October 2004 (04.10.2004)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse